

## PATENT ABSTRACTS OF JAPAN

(11)Publication number : 2001-023297

(43)Date of publication of application : 26.01.2001

(51)Int. Cl.

G11B 20/10

G06F 12/14

G08C 5/00

G11B 27/00

(21)Application number : 11-189023

(71)Applicant : SHARP CORP

(22)Date of filing : 02.07.1999

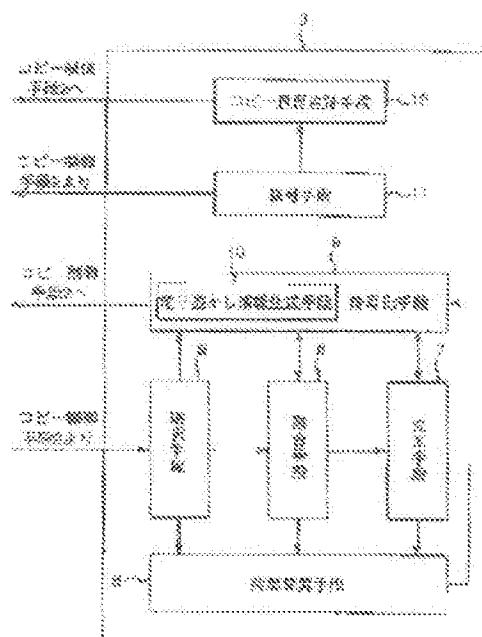
(72)Inventor : KUGA SHIGEKI

(54) CONTENTS DISTRIBUTION CONTROL DEVICE AND PROGRAM RECORDING MEDIUM

(57)Abstract.

PROBLEM TO BE SOLVED: To make it possible to inhibit illegal copy, and to ascertain the source of the illegal copy.

SOLUTION: When the ID of a copy requesting device is not registered in copy limitation information, a copy control means rejects the request for copy judging it as illegal. A copy history tracing means 12 of the contents distribution control information recording means 3, while comparing the history of contents DNA accumulated in the contents with the original contents DNA of the copying device, performs inverse procedures of harmonization by a harmonization means 6 and crossing by a crossing means 7 until it finally arrives at the original contents DNA of said contents. Thus, the source of the illegal copy is ascertained by extracting the original contents DNA of the copy device which has copied said contents.





(10) 日本国特許庁 (J P)

(12) 公開特許公報 (A)

(11) 特許出願公開番号  
特開2001-23297  
(P2001-23297A)

(43) 公開日 平成13年1月26日 (2001.1.26)

(51) Int.Cl. <sup>7</sup>	識別記号	F I	シ-ネ-ジ (参考)
G 1 1 B 20/10		G 1 1 B 20/10	H 5 B 0 1 7
G 0 6 F 12/14	3 2 0	G 0 6 F 12/14	3 2 0 E 5 D 0 4 4
G 0 9 C 5/00		G 0 9 C 5/00	5 D 1 1 0
G 1 1 B 27/00		G 1 1 B 27/00	5 J 1 0 4
			A 9 A 0 0 1

審査請求 未請求 請求項の数12 O L (全 19 頁)

(21) 出願番号 特願平11-180023  
(22) 出願日 平成11年7月2日 (1999.7.2)

(71) 出願人 000085649  
シャープ株式会社  
大阪府大阪市阿倍野区長池町22番22号  
(72) 発明者 空閑 茂樹  
大阪府大阪市阿倍野区長池町22番22号 シャ  
ープ株式会社内  
(74) 代理人 100002144  
弁理士 青山 徹 (外1名)

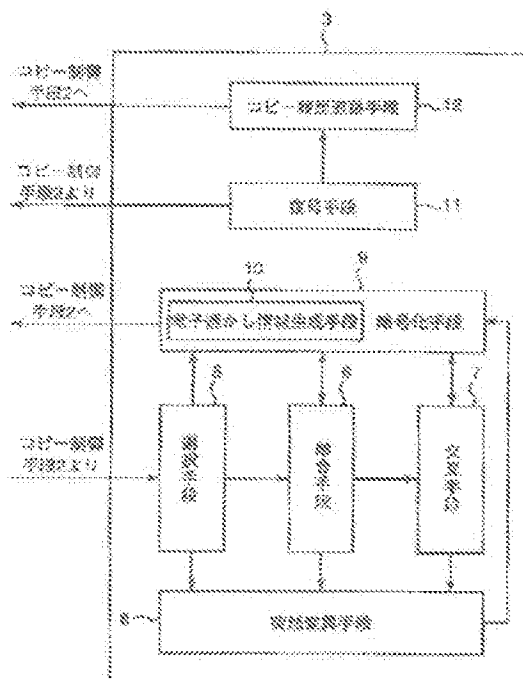
最終頁に続く

(54) 【発明の名称】 コンテンツ流通管理装置およびプログラム記録媒体

(57) 【要約】

【課題】 不正コピーを禁止し、不正コピーの発生を検知させる。

【解決手段】 コピー制御手段は、要求コピー装置のIDがコピー制御情報に登録されているか検査し、当該コピー要求が不正であるとしてコピー拒否を行う。コンテンツ流通管理情報記録手段3のコピー制御情報手段12は、コンテンツに關聯されているコンテンツDNAの登録とコピー装置のオリジナルコンテンツDNAとの比較を行いながら、当該コンテンツのオリジナルコンテンツDNAに適用するまで融合手段6による融合と交叉手段7による交叉の連続の手順を行う。こうして、当該コンテンツをコピーしたコピー装置のオリジナルコンテンツDNAを抽出して、不正コピーの発生を検知させる。



## 【特許請求の範囲】

【請求項 1】 コンテンツあるいはコンテンツの流通管理に関する情報を記憶する記憶手段と、

上記コンテンツのコピー実行を制御するコピー制御手段と、

上記コンテンツの属性を表す情報及びコピー主体の属性を表す情報であって、コピー履歴情報として機能できるコンテンツ流通管理情報を生成して、コピー元およびコピー先の両コンテンツのコピー対象領域に記憶するコンテンツ流通管理情報記憶手段を備えたことを特徴とするコンテンツ流通管理装置。

【請求項 2】 請求項 1 に記載のコンテンツ流通管理装置において、

上記コンテンツ流通管理情報記憶手段は、上記コンテンツ流通管理情報を多重化して記憶するようになっていて、これを特徴とするコンテンツ流通管理装置。

【請求項 3】 請求項 2 に記載のコンテンツ流通管理装置において、

上記コンテンツ流通管理情報記憶手段は、コピー実行の際に、上記コンテンツのコピー対象領域に多重化されて記憶されているコンテンツ流通管理情報から一画の情報を選択して読み出す選択手段と、

上記選択された一画の情報と、コピーを行うコピー主体の属性を表す情報とに基づいて、多重化された新たなコンテンツ流通管理情報を生成する融合手段を備えていることを特徴とするコンテンツ流通管理装置。

【請求項 4】 請求項 3 に記載のコンテンツ流通管理装置において、

上記融合手段によって生成されたコンテンツ流通管理情報を構成する対を成す情報間で情報の一部を交換する交叉を行う交叉手段を備えて、

上記コンテンツ流通管理情報記憶手段は、上記交叉されたコンテンツ流通管理情報を記憶することを特徴とするコンテンツ流通管理装置。

【請求項 5】 請求項 4 に記載のコンテンツ流通管理装置において、

上記交叉手段は、予め設定された交叉回数に基づいて、上記対を成す情報間における交叉の位置、交叉の幅および交叉の発生頻度を制御するようになっていて、これを特徴とするコンテンツ流通管理装置。

【請求項 6】 請求項 1 に記載のコンテンツ流通管理装置において、

上記生成されたコンテンツ流通管理情報の一部を変換させる突然変異手段を備えて、

上記コンテンツ流通管理情報記憶手段は、上記変換されたコンテンツ流通管理情報を記憶することを特徴とするコンテンツ流通管理装置。

【請求項 7】 請求項 6 に記載のコンテンツ流通管理装置において、

上記突然変異手段は、予め設定された突然変異回数に基

づいて、上記変異の位置、変異の幅および変異の発生頻度を制御するようになっていて、これを特徴とするコンテンツ流通管理装置。

【請求項 8】 請求項 1 に記載のコンテンツ流通管理装置において、

上記コンテンツのコピー対象領域は、当該コンテンツの構成に関連する単位であることを特徴とするコンテンツ流通管理装置。

【請求項 9】 請求項 1 に記載のコンテンツ流通管理装置において、

上記コンテンツのコピー対象領域に記憶されているコンテンツ流通管理情報において、コピーの履歴を追跡してコピー主体を特定するコピー履歴追跡手段を備えたことを特徴とするコンテンツ流通管理装置。

【請求項 10】 請求項 1 に記載のコンテンツ流通管理装置において、

上記記憶手段における記憶命令では読み出せない特定領域には、各コンテンツ毎に、コピーが許可されたコピー主体の情報を含むコピー制限情報が記憶されており、

上記コピー制御手段は、コピーを実行する前に上記コピー制限情報を参照し、要求コピー主体が上記コピー制限情報に記録されているコピー主体である場合にのみ上記コンテンツ流通管理情報記憶手段に上記コンテンツ流通管理情報の生成を指示し、

上記コンテンツ流通管理情報記憶手段は、上記命令に基づいて上記コンテンツ流通管理情報を生成するようになっていて、これを特徴とするコンテンツ流通管理装置。

【請求項 11】 請求項 10 に記載のコンテンツ流通管理装置において、

上記コピー制御手段は、上記要求コピー主体が上記コピー制限情報に登録されていないコピー主体である場合には、コピーの実行を禁止するかあるいはコピー禁止マークを表示することを特徴とするコンテンツ流通管理装置。

【請求項 12】 コンピュータを、記憶手段における記憶命令では読み出せない特定領域に、各コンテンツ毎に、コピーが許可されたコピー主体の情報を含むコピー制限情報を格納する情報格納手段と、

コンテンツの属性を表す情報およびコピー主体の属性を表す情報であって、コピー履歴情報として機能できるコンテンツ流通管理情報を生成するコンテンツ流通管理情報生成手段と、

上記生成されたコンテンツ流通管理情報を構成する対を成す情報間において情報の一部を交換する交叉を行う交叉手段と、

上記生成されたコンテンツ流通管理情報の一部を変換させる突然変異手段と、

上記生成されたコンテンツ流通管理情報を符号化する符号化手段と、

上記番号化されたコンテンツ使用管理情報に基づいて電子選考し情報生成してコピー元およびコピー先の両コンテンツのコピー対象領域に記録する電子選考し情報生成手段と、

上記コンテンツに記録されているコンテンツ使用管理情報を復号化する復号手段と、

上記復号化されたコンテンツ使用管理情報に基づいて、コピーの複製を意味してコピー主体を特定するコピー複製判断手段と、

要求コピー主体が上記コピー制限情報に登録されているコピー主体である場合にのみ上記コンテンツのコピーを実行するコピー制御手段として機能させるコンテンツ流通管理処理プログラムおよびコピー履歴記録処理プログラムが記録されたことを検出するコンピュータ読出し可能なプログラム記録媒体。

【発明の詳細な説明】

【0001】

【発明の属する技術分野】 本発明は、デジタル・コンテンツ（以下、単にコンテンツと書く）のコピーの主体を任意のコンテンツのコピーの対象をコンテンツ流通管理情報としてコンテンツ内に記録し、コンテンツの不正コピーの防止またはコンテンツのコピー履歴からコピー主体を識別するコンテンツ流通管理装置に関する。

【0002】

【従来の技術】 最近、デジタル・コンテンツの普及に伴って、コンテンツがネットワークあるいは記録媒体を介して不正にコピーされて普及していく傾向にある。そこで、固有の記録媒体あるいはコンテンツ自身に複製団体やワーキング・グループ等を設立して、不正コピーの防止策が考案されている。

【0003】 例えば、「高橋典彦、池見源一郎、1998.3.23(日) 日経B P社、日経エレクトロニクス 1998.3.23(日) 6,7(2) pp. 47~pp. 53」には、1998.3.23(日)のコピー防止法として、CPTWG（コピー・プロテクション・テクニカル・ワーキング・グループ）に提案された以下に示すような第1の不正コピーの防止技術が記載されている。

【0004】 即ち、先ず、コンテンツにCCI（コピー・コントロール・インフォメーション）と呼ばれる情報を埋め込む。次に、ユーザからのコピーの要求があると、コンテンツを送信する送信側の場合は、上記CCIを参照してコピーが可能か否かを調べる。ここで、CCIは2ビットの情報から成り、2ビットの値によって「コピー不可」、「一度だけコピー可能」、「これ以上のコピーを認めない」および「何回でもコピー可能（コピー許可）」の4種類に意味付けられている。

【0005】 次に、上記送信側の機器は、受信側の機器がコピー防止技術を実行しているかどうかを確認する確認を行う。尚、上記確認には、完全確認と照合付確認と

がある。そして、送信側と受信側との双方が公認値を行っている場合は、完全確認成立とする。尚、上記完全確認においては、コピーが認められていないコンテンツのデータも送信するように制御する。これに対して、上記照合付確認においては、コピーが認められた場合、すなわち上記CCIの内容が「一度だけコピー可能」および「何回でもコピー可能」の場合のみコンテンツを送信するように制御する。

【0006】 ここで、コピーが認められたコンテンツは暗号化せずにデータを送り出しても良いが、コピーが認められていないデータを送受信する場合は、必ず暗号化が必要になっている。そして、暗号化されたコンテンツは、公開鍵によって復号化を行うことになる。

【0007】 また、第2の不正コピーの防止技術として、上記CPTWGでは、DVD（デジタル・ビデオ・ディスク）に関して、CSS（コンテンツ・スクランブラング・システム）を採用している。このCSSでは、4種類のコピー防止策が施されている。一つ目の防止策は、コンテンツ番号化と呼ばれるもので、「マスターキー」、「ディスクキー」および「タイトルキー」という三つの暗号化鍵を組み合わせてコンテンツを暗号化する。その場合、上記「ディスクキー」および「タイトルキー」は、コンテンツと共にパーソナルコンピュータ（以下、パソコンと略称する）等の固定ファイルシステムを介して読み出せないDVDの領域に埋め込まれている。

【0008】 二つ目の防止策は、リージョナルコードによる再生制限である。これはDVD装置を販売した地域のリージョナルコードをDVD装置の回路やファームウェアに埋め込むことにより実現される。

【0009】 三つ目の防止策は、AFS（アナログ・プロテクション・システム）である。このAFSは、アナログVTR（ビデオ・テープ・レコーダ）等に刻するコピー制限を行うためのものであり、テレビ映像信号の出力回路にハードウェアで組み込んで用いられている。

【0010】 四つ目の防止策は、パス認証によるコピー防止策であり、パソコン等に搭載されたDVD装置に特有の処理技術である。このパス認証においては、DVD装置とCSSキジュール（あるいはDVD復号化ボード）によって、相手はCSSライセンスを受けているか否かを確認し、相手がCSSライセンスを受けていると分かるまでデータ転送を行わないようにしている。その場合、DVD装置とCSSキジュールとは、「パスキー（Pass Key）」という毎回変わる暗号化鍵データを共有している。そして、上記DVD装置からCSSキジュールに上記「ディスクキー」や「タイトルキー」を送信する場合には、「パスキー」で暗号化してから転送することによって「ディスクキー」や「タイトルキー」の盗聴を防ぐようになっている（ソフトウェア技術者の力を得る不正コピー防止技術にメド）、日経B P社、日経エレクトロニクス、1997.2.18(No. 690) pp. 119~pp. 120。

【0011】また、第3の不正コピーの防止技術として、特開平9-191394号の項に開示された、オーディオ、画像、映像あるいはマルチメディアデータに電子透かしを挿入する技術がある。同公報によれば、画像、オーディオ信号あるいは映像のシーケンスを処理してはスペクトラム周波数分解で分解し、分解部分の如意的に重要な成分中に透かしの識別子を埋め込むことで電子透かしを實現している。

【0012】一方において、動植物のDNA(デオキシリボ核酸:遺伝物質の一つ)から動植物のルーンを特定する技術が知られている。例えば、『開山寺大著“DNAで何が分かるか”講談社ブルーバックス、1995』には、DNAから骨を成すに基いて人類のルーンであるイブを特定することが記載されている。また、遺伝子に関する交叉や突然変異の人工的な発生方法に関しては『メラニー・スニッチェル著“遺伝的アルゴリズムの技法”東京電気大学、1997』等に記載されている。

【0013】

【発明が解決しようとする課題】しかしながら、上記従来の不正コピーの防止技術には、以下のような問題がある。すなわち、先ず、上記第1、第2の不正コピーの防止技術においては、不正コピーの防止を目的としてはいるものの、一旦不正コピー防止策が実行されると無制限に不正コピーが実行される可能性があるという問題がある。さらに、不正コピーを防止することに主眼が置かれ、不正コピーが行われた場合には不正コピーの発生原因どこに在るかを突き止めることができないという問題もある。さらには、コピー防止に係わる情報をパソコン等の論理ファイルシステムを介して読み書きなり記憶に埋め込んで仕舞うが、例えばマイクロプロセッサのIC IC E(インサーキット・ロム・メモリー)やロジックアナライザ等を使うと読み出すことも可能であり、専門知識を有する人に対する不正コピーの防止は万全でないという問題がある。

【0014】また、上記第1の不正コピーの防止技術においては、一つのコンテンツに一つのIC Iが割り付けられているため、一つのコンテンツにおける部分的な不正コピーに対しては全く耐性が無いという問題がある。尚、上記第1の不正コピーの防止技術においては、不正コピーのアルゴリズムをハードウェアとして実装する方法が取られようとしている。ところが、この場合においても、例えば、暗号解読用LS I(大規模集積回路)と映像等の復号化用LS Iとの間を結ぶバレルリンクウェーブにロジックアナライザを当て、暗号解読後のデータストリームを盗むことができる。あるいは、復号化LS IとデマルチプレクサをラレータLS Iとを結ぶ映像伝送用の専用バスに、映像キャプチャボードを接続すれば、容易に不正コピーを行うことができるという問題がある。

【0015】一方、上記第3の不正コピーの防止技術に

おいては、不正コピーされたコンテンツの品質を極端に落とすことはできるものの、不正コピーそのものを禁止することはできないという問題がある。さらには、上記第1、第2の不正コピーの防止技術の場合と同様に、不正コピーが行われた場合に、その発生源に拘わる情報を得ることができないという問題がある。

【0016】ところで、上記DNAは、動植物の種やルーンを特定するのに有効な情報の一つである。ところが、DNAのような情報をコンテンツの流通やコピー管理の情報として利用する技術については未だ公知されてはいない。

【0017】そこで、この発明の目的は、不正コピーを禁止すると共に、不正コピーが行われた場合にはその発生源を突き止めることができるコンテンツ流通管理装置、および、コンテンツ流通管理プログラムが記録されたプログラム記録媒体を提供することにある。

【0018】

【課題を解決するための手段】上記目的を達成するため、第1の発明のコンテンツ流通管理装置は、コンテンツあるいはコンテンツの流通管理に係わる情報を記録する記録手段と、上記コンテンツのコピー実行を制御するコピー制御手段と、上記コンテンツの属性を表す情報およびコピー主体の属性を表す情報であって、コピー属性情報として機能できるコンテンツ流通管理情報を生成して、コピー元およびコピー先の両コンテンツのコピー対象領域に記録するコンテンツ流通管理情報記録手段を備えたことを特徴としている。

【0019】上記構成によれば、コピー制御手段によってコンテンツのコピーが許可されると、コンテンツ流通管理情報記録手段によってコンテンツ流通管理情報が生成されて上記コンテンツのコピー対象領域に記録される。したがって、不正にコピーされたコンテンツあるいはそのコピー対象領域に記録されているコンテンツ流通管理情報に基づいて、コピーの履歴を追跡してコピー主体を特定することが可能となる。こうして、不正コピーの発生源を突き止めることができる。

【0020】また、上記第1の発明における上記コンテンツ流通管理情報記録手段は、上記コンテンツ流通管理情報を多重化して記録することが望ましい。

【0021】上記構成によれば、上記コンテンツの属性を表す情報と上記コピー主体の属性を表す情報とを多重化して1つのコンテンツ流通管理情報とすることが可能となる。したがって、上記コンテンツ流通管理情報を解析することによって、上記コンテンツとコピー主体との関係が解明される。

【0022】また、上記第1の発明は、上記コンテンツ流通管理情報記録手段に、コピー実行の際に、上記コンテンツのコピー対象領域に多重化されて記録されているコンテンツ流通管理情報から一意の情報を選択して読み出す選択手段と、上記選択された一意の情報と、コピー

7

を行うコピー主体の属性を表す情報とに基づいて、多量化された新たなコンテンツ流通管理情報を生成する融合手段を備えることが望ましい。

【0023】上記構成によれば、上記コンテンツの属性を表す情報と上記コピー主体の属性を表す情報とが多量化されて1つのコンテンツ流通管理情報が生成される。したがって、上記コンテンツ流通管理情報を解析することによって、何れのコンテンツが何れのコピー主体によってコピーされたかが容易に解明される。

【0024】その際、上記融合に生成されたコンテンツ流通管理情報は、上記コンテンツのコピー対象領域に記録されている元のコンテンツ流通管理情報と同じ情報を有している。したがって、コピー操作が繰り返されても上記情報量が一定に保たれて、コピーの履歴情報が増えることはない。

【0025】また、上記第1の発明は、上記融合手段によって生成されたコンテンツ流通管理情報を構成する対を成す情報間で情報の一部が交換される交叉を行う交叉手段を備えて、上記コンテンツ流通管理情報記録手段は、上記交叉されたコンテンツ管理流通情報を記録することが望ましい。

【0026】上記構成によれば、上記コンテンツがコピーされてコンテンツ流通管理情報が生成される度に、対を成す情報間で情報の一部が交換される。その結果、上記コンテンツ流通管理情報を構成する対を成す情報の何れか一方には、現在までコピーに関わったコピー主体の属性を表す情報が導入される。

【0027】また、上記第1の発明における上記交叉手段は、予め設定された交叉間数に基づいて、上記対を成す情報間における交叉の位置、交叉の幅および交叉の発生頻度を制御するようになっていたことが望ましい。

【0028】上記構成によれば、現在までコピーに関わった総てのコピー主体の属性を表す情報が失われることなく上記コンテンツ流通管理情報に導入され、且つ、内容が不連続になるように、上記交叉の位置、交叉の幅および交叉の発生頻度が制御される。

【0029】また、上記第1の発明は、上記生成されたコンテンツ流通管理情報の一部を変異させる突然変異手段を備えて、上記コンテンツ流通管理情報記録手段は、上記変異されたコンテンツ管理流通情報を記録することが望ましい。

【0030】上記構成によれば、上記コンテンツ流通管理情報の内容が攪乱されて、上記コンテンツ流通管理情報の内容が外部に漏れることが防止される。

【0031】また、上記第1の発明における上記突然変異手段は、予め設定された突然変異間数に基づいて、上記変異の位置、変異の幅および変異の発生頻度を制御するようになっていたことが望ましい。

【0032】上記構成によれば、上記コンテンツ流通管理情報の内容がより効果的に攪乱されるように、上記変

8

異の位置、変異の幅および変異の発生頻度が制御される。

【0033】また、上記第1の発明における上記コンテンツのコピー対象領域は、当該コンテンツの構造に関連する単位であることが望ましい。

【0034】上記構成によれば、コンテンツの構造に関連する単位で上記コンテンツ流通管理情報が記録される。したがって、コンテンツの部分単位でコピーに対しても効果が発揮される。

【0035】また、上記第1の発明は、上記生成されたコンテンツ流通管理情報を暗号化する暗号化手段を備えて、上記コンテンツ流通管理情報記録手段は、上記暗号化されたコンテンツ管理流通情報を記録することが望ましい。

【0036】上記構成によれば、上記コンテンツ流通管理情報の内容が攪乱・隠蔽されて、上記コンテンツ流通管理情報の内容が外部に漏れることが効果的に防止される。

【0037】また、上記第1の発明は、上記暗号化されたコンテンツ流通管理情報に基づいて電子透かし情報を生成する電子透かし情報生成手段を備えて、上記コンテンツ流通管理情報記録手段は、上記電子透かし情報を記録することが望ましい。

【0038】上記構成によれば、上記コンテンツ流通管理情報の内容がより完全に攪乱・隠蔽されて、上記コンテンツ流通管理情報の内容が外部に漏れることが更に効果的に防止される。

【0039】また、上記第1の発明は、上記コンテンツのコピー対象領域に記録されているコンテンツ流通管理情報に基づいて、コピーの履歴を追跡してコピー主体を特定するコピー履歴追跡手段を備えることが望ましい。

【0040】上記構成によれば、不正にコピーされたコンテンツあるいはそのコピー対象領域に記録されているコンテンツ流通管理情報に基づいて、コピー履歴追跡手段によって、コピーの履歴が追跡されてコピー主体が特定される。こうして、不正コピーの発生頻度が容易に突き止められる。

【0041】また、上記第1の発明は、上記コンテンツのコピー対象領域に記録されているコンテンツ流通管理情報を復号化する復号手段と、上記復号化されたコンテンツ流通管理情報に基づいて、コピーの履歴を追跡してコピー主体を特定するコピー履歴追跡手段を備えることが望ましい。

【0042】上記構成によれば、不正にコピーされたコンテンツあるいはそのコピー対象領域に記録されているコンテンツ流通管理情報が暗号化されていても、コピー履歴追跡手段によって、コピーの履歴が追跡されてコピー主体が特定される。

【0043】また、上記第1の発明は、上記記憶手段における論理命令では読み出せない特定領域には、各コン

テンツ毎に、コピーが許可されたコピー主体の情報を含むコピー制限情報を記憶し、上記コピー制御手段は、コピーを実行する前に上記コピー制限情報を参照して、要求コピー主体が上記コピー制限情報に登録されているコピー主体である場合にのみ上記コンテンツ流通管理情報記憶手段に上記コンテンツ流通管理情報の生成を指令し、上記コンテンツ流通管理情報記憶手段は、上記指令に基づいて上記コンテンツ流通管理情報を生成するようにすることが望ましい。

【0044】上記構成によれば、上記コピー制御手段によって、コピー要求を出しているコピー主体がコピー許可対象のコピー主体である場合にコピーが許可される。こうして、コピー許可対象ではないコピー主体からの不正コピーが防止される。さらに、上記コピー制限情報は、論理命令では読み出せない特定領域に記憶されているので、通常のコピー命令で読み出して改ざんすることは不可能である。

【0045】また、上記第1の発明における上記コピー制御手段は、上記要求コピー主体が上記コピー制限情報に登録されていないコピー主体である場合には、コピーの実行を禁止するかあるいはコピー禁止メッセージを表示することが望ましい。

【0046】上記構成によれば、上記コピー制御手段によって、コピー要求を出しているコピー主体がコピー許可対象ではないコピー主体である場合に、コピーの実行が禁止される。こうして、コピーが許可されていないコピー主体からの不正コピーが防止される。

【0047】また、第2の発明のプログラム記憶媒体は、コンピュータを、記憶手段における論理命令では読み出せない特定領域に、各コンテンツ毎に、コピーが許可されたコピー主体の情報を含むコピー制限情報を格納する情報格納手段と、コンテンツの属性を表す情報およびコピー主体の属性を表す情報であって、コピー履歴情報として機能できるコンテンツ流通管理情報を生成するコンテンツ流通管理情報生成手段と、上記生成されたコンテンツ流通管理情報を格納する格納手段において情報の一部を交換する交叉を行う交叉手段と、上記生成されたコンテンツ流通管理情報の一部を交換させる交換実行手段と、上記生成されたコンテンツ流通管理情報を暗号化する暗号化手段と、上記暗号化されたコンテンツ流通管理情報に基づいて電子透かし情報生成してコピー元およびコピー先の両コンテンツのコピー対象領域に記録する電子透かし情報生成手段と、上記コンテンツに登録されているコンテンツ流通管理情報を復号化する復号手段と、上記復号化されたコンテンツ流通管理情報に基づいて、コピーの履歴を追跡してコピー主体を特定するコピー履歴追跡手段と、要求コピー主体が上記コピー制限情報に登録されているコピー主体である場合にのみ上記コンテンツのコピーを実行するコピー制御手段として機能させるコンテンツ流通管理処理プログラムおよびコ

ピー履歴追跡処理プログラムが記録されたことを特徴としている。

【0048】上記構成によれば、上記コンテンツがコピーされてコンテンツ流通管理情報が生成される際に、上記コンテンツ流通管理情報には現在までコピーに内わたったコピー主体の属性を表す情報が挿入される。したがって、不正にコピーされたコンテンツまたはそのコピー対象領域に登録されているコンテンツ流通管理情報に基づいて、コピーの履歴を追跡されてコピー主体が特定される。こうして、不正コピーの発生源が容易に突き止められる。さらに、上記コンテンツ流通管理情報の内容が盗取・漏洩されて、上記コンテンツ流通管理情報の内容が外部に漏れることが効果的に防止される。さらに、コピー要求を出しているコピー主体がコピー許可対象ではないコピー主体である場合の不正コピーが防止される。

【0049】

【発明の実施の形態】以下、この発明の図示の実施の形態により詳細に説明する。図1は、本実施の形態のコンテンツ流通管理装置におけるブロック図である。記憶手段1には、コンテンツ、コンテンツ流通管理情報およびコピー制限情報が記憶されている。この記憶手段1は、FD(フロッピーディスク)、CD-R(コンパクトディスク)、MO(磁気光ディスク)、DVD、ハードディスク等の記憶メモリ、あるいは、RAM(ランダムアクセスメモリ)、スマートカード、フラッシュメモリ等の半導体メモリなどで実現される。

【0050】コピー制御手段2は、上記コンテンツのコピー可否の判断やコピー実行を制御する。コンテンツ流通管理情報記憶手段3は、コンテンツあるいはコンテンツをコピーする主体であるコピー装置4のコンテンツ流通管理情報を読み込み、後に詳述する選択手段、融合手段、交叉手段、交換実行手段及び暗号化手段を用いて新たなコンテンツ流通管理情報を生成する。そして、コピー制御手段2を介して、コピー元及びコピー先の両コンテンツに書き込むと共に、コピー元のコンテンツはコピー装置4に送出する。さらに、生成したコンテンツ流通管理情報自体とコピー装置4のコンテンツ流通管理情報とを記憶手段1に記憶・蓄積する。また、コピーされたコンテンツに書き込まれたコンテンツ流通管理情報に基づいてコピー履歴を追跡する。コピー装置4は、コンテンツあるいはコンテンツの一部のコピー要求をコピー制御手段2に対して行い、コピー制御手段2の制御に基づいて複製したコンテンツをコピーする。

【0051】尚、上記コピー制御手段2およびコンテンツ流通管理情報記憶手段3は、専用のLSIまたはICP(中央演算処理装置)で実現することが可能である。また、コピー装置4は、コピー実行が可能なLSI、ICP、パソコンおよび端末装置等で実現される。コピー装置4は、本コンテンツ流通管理装置内部に含まれてもよいし、本コンテンツ流通管理装置とは別の装置で構成し



でも差し支えない。あるいは、コピー装置4を除く記録手段1、コピー装置2およびコンテンツ流通管理情報記録手段3は、他の装置のCPU等を利用することも可能である。

【0052】図2は、この発明の特徴であるコンテンツ流通管理情報記録手段3の内部構成を示す。コンテンツ流通管理情報記録手段3は、選択手段5、融合手段6、交叉手段7、突然変異手段8、暗号化手段9、復号手段11およびコピー装置2と接続手段12で構成される。

【0053】上記選択手段5は、本コンテンツ流通管理装置あるいはコピー装置4で二重化されているコンテンツ流通管理情報の一方を選択することによって、一重の情報に変換する。尚、本実施の形態においては、上記コンテンツ流通管理情報は二重化された情報であるとして説明するが、二重以上に多重化された場合であっても適用可能である。

【0054】上記融合手段6は、上記選択手段5で選択されたコピー装置4のコンテンツ流通管理情報と、コピー対象となるコンテンツのコンテンツ流通管理情報とを融合する。そして、新たな二重化されたコンテンツ流通管理情報を生成する。交叉手段7は、融合手段6によって二重化されたコンテンツ流通管理情報において互いの情報の一欄を交換する。突然変異手段8は、上記コンテンツ流通管理情報の一部の値あるいは全部の値を回転させる。尚、本実施の形態においては、コンテンツ流通管理情報がコンテンツあるいはコンテンツを記録した記録手段1の中にそのコピーの履歴を残しながら変換していくことから、以後、コンテンツ流通管理情報のことをコンテンツDNAあるいは単にDNAと略称する場合がある。

【0055】上記暗号化手段9は、上記選択手段5、融合手段6、交叉手段7あるいは突然変異手段8に対するコンテンツ流通管理情報の入力または出力の段階で、コンテンツ流通管理情報(コンテンツDNA)に対して暗号化を行う。また、上記暗号化は上記各手段5〜8に關して強制であってもよい。尚、上記暗号化の課題はこの発明の対象ではない。また、変換手段10を有して、暗号化されたコンテンツDNAに基づいて電子透かし情報を生成する。

【0056】上記復号手段11は、上記暗号化手段9で暗号化され、電子透かし情報生成手段10で電子透かし情報化されたコンテンツDNAを復号化する。また、コピー装置2の接続手段12は、復号化されたコンテンツDNAに基づいて、コンテンツがどのような順序でコピーされたか、コピーの主体は誰であるか、等のコピー履歴を記録する。この履歴に關しては後に詳述する。

【0057】図3は、上記コンテンツDNAおよびその暗号化の一側面を示す。図3(a)は、コンテンツDNAの一側であり、コンテンツあるいはコピー装置4の属性あるいはID(識別子)を表す記号列である。尚、図3(a)

では、コンテンツあるいはコピー装置4のID番号を上記記号列として用いた場合の例を示しているが、番号に換わることも特定記号や特定のキーワード等であっても何ら差し支えない。

【0058】図3(b)は、上記暗号化手段9によって、図3(a)に示すコンテンツDNAを暗号化した結果を示す。この暗号化は、暗号化手段9が保有する方式の関数に基づいて生成した鍵を用いて行われる。但し、図3(b)においては、得られた暗号を直接書き出すと8ビット単位で文字列に変換して表示している。図3(c)は、今後の説明を簡単にするために、図3(b)に示す文字列の最初の部分を切り出したものである。以後、図3(d)の文字列を、短縮化されたコンテンツDNAを表す情報の全体を代表するものとして説明を行う。尚、説明の便宜上、上記暗号を8ビット単位で変換した文字列をコンテンツDNAとして扱う。また、図3(d)は、図3(c)のコンテンツDNAが二重化されて保存されることを示している。

【0059】図4は、上記融合手段6による融合、交叉手段7による交叉および突然変異手段8による突然変異におけるコンテンツDNAの変遷を示す。図4(a)は二重化されたコンテンツDNAを示す。ここで、21は、コンテンツ側のコンテンツDNAである。また、22は、コンテンツDNA21と同様に生成されたコピー装置4側のコンテンツDNAである。図4(a)の場合、コンテンツ側およびコピー装置4側双方のコンテンツDNAは、互いに同じ情報が二重に記録されている状態を示している。

【0060】図4(b)は、上記選択手段5によって、二重化されたコンテンツ側のコンテンツDNA21の何れか一方、および、二重化されたコピー装置4側のコンテンツDNA22の何れか一方が選択され、融合手段6によって、上記選択されたコンテンツ側のコンテンツDNA23とコピー装置4側のコンテンツDNA24とで二重化された新たなコンテンツDNAが生成された状態を示す。

【0061】図4(c)は、上記融合手段6によって生成された新たなコンテンツDNAの側に対して、交叉手段7によって交叉が行われた状態を示す。この場合の交叉は、図4(b)に示すコンテンツ側のコンテンツDNA23とコピー装置4側のコンテンツDNA24とにおける互いの左端から5文字同士を入れ換えることによって行われる。以後、このように部分文字列を入れ換えることを「交叉する」と言う。つまり、コンテンツDNA23の左端から5文字がコンテンツDNA24の左端から5文字に交叉したものがコンテンツDNA25であり、逆にコンテンツDNA24の左端から5文字がコンテンツDNA23の左端から5文字に交叉したものがコンテンツDNA26である。

【0062】図4(d)は、上記突然変異手段8によって

13

突然変異が行われた状態を示す。この場合の突然変異は、図4(a)に示すコンテンツDNA23の一部の情報突然変化して、コンテンツDNA27となった状態である。この場合には、「文字列Z」なる部分情報が「文字列Y」なる情報に変化している。

【0063】図5は、上記コンテンツDNAに対して上記交叉が行われた状態を表す概念図である。上記交叉の種類には1点交叉、2点交叉、一価交叉等があるが、本実施形態においては、特に交叉の種類は問わない。本実施形態においては、一例として2点交叉の場合を説明する。「交叉1」は、あるコンテンツDNAの一部の領域の情報が対になっているコンテンツDNAの対応する領域の情報と入れ替わることによって行われる。

【0064】図5において、31は、交叉が行われた後のコンテンツDNAを示している。そして、コンテンツDNA31中における情報32および情報34は、元のコンテンツDNAの情報である。また、斜線を施した情報33は、交叉によって対になっているコンテンツDNAから入れ替えられた情報である。

【0065】ここで、上記情報33が、コンテンツDNA31の左端から1 $\phi$ の位置に1 $\phi$ の幅を有して交叉する確率 $p_1$ は、交叉そのものが発生する確率を $p_+$ とし、交叉情報が幅1 $\phi$ を持つ確率を $p_\phi$ とし、交叉が左端から1 $\phi$ の位置に発生する確率を $p_1$ とすると、「 $p_+ = p_+ \cdot p_\phi \cdot p_1$ 」であることができる。同様に、上記突然変異も確率 $p_+$ で発生する。尚、交叉及び突然変異が発生する確率 $p_+$ 、 $p_\phi$ は、交叉手段7内および突然変異手段8内の確率発生器によって発生される。

【0066】図6は、上記コピー制御手段2の制御の下に、上記コンテンツ流通管理情報記憶手段3によって実行されるコンテンツ流通管理情報記憶処理動作のフローチャートである。以下、図6に従って、コンテンツ流通管理情報記憶処理について説明する。

【0067】ステップS1で、上記コピー制御手段2によって、コピー装置4からのコピー要求があるか否かが判別される。そして、コピー要求があるとステップS2に進む。ここで、上記コピー要求は、コンテンツ全体に対して行われる場合とコンテンツの一部に対して行われる場合とがあるが、説明を簡単にするために、ここではコンテンツ全体に対して行う場合を例に説明する。尚、コンテンツの一部に対してコピー要求を行う場合については、後に補足説明を行う。

【0068】ステップS2で、上記コピー制御手段2によって、コンテンツDNAの照会が行われる。照会されるコンテンツDNAは、コンテンツ側とコピー要求を送出したコピー装置4側との双方のコンテンツDNAである。尚、少なくともコンテンツ側のコンテンツDNAは、図3(a)に示すような形式でコンテンツに書き込まれて記憶手段1に記憶されている。これに対して、コ

14

ピ化されている必要はなく、例えば、図3(a)または図3(b)に示すような形式の情報であっても差し支えない。

【0069】ステップS3で、上記コピー制御手段2によって、コンテンツ側に書き込まれて記憶されているコンテンツDNAとコピー装置4側のコンテンツDNAとに於いて、コンテンツあるいは記憶手段1から読み出されたコピー適合条件に基づいて、コピーの可否が判別される。そして、コピー可である場合にはステップS4に進み、コピー不可である場合にはステップS13に進む。

尚、このコピー可否の判別については別途述べる。

【0070】ステップS4で、上記コピー制御手段2からのコピー許可指示に応じて、コンテンツ流通管理情報記憶手段3の選択手段5によって、多重化されたコンテンツ側のコンテンツDNAの中から一つが選択され、コンテンツDNAが一重化される。尚、多重化されている各コンテンツDNA同士は必ずしも同一の情報ではなく、コピーの世代を重ねて行くに従って内容情報は異なっているものである。

【0071】ステップS5で、上記選択手段5によって、ステップS4において一重化されたコンテンツ側のコンテンツDNAをコピー装置4側のコンテンツDNAと組み合わせ、多重化したコンテンツDNAを生成する組合処理が行われる。

【0072】ステップS6で、上記交叉手段7によって、コンテンツDNAの交叉確率パラメータが生成される。ここで、上記交叉確率パラメータとしては、上述した交叉発生確率 $p_+$ 、位置の確率 $p_1$ 、幅確率 $p_\phi$ が用いられる。ステップS7で、交叉手段7によって交叉処理が行われる。すなわち、ステップS6において生成された確率パラメータに基づいて、交叉の位置と幅とが決定され、発生確率 $p_+$ に従って二重化(多重化)されたコンテンツ側のコンテンツDNAとコピー装置4側のコンテンツDNAとの間で交叉が実行される。

【0073】ステップS8で、上記突然変異手段8によって、コンテンツDNAの突然変異パラメータが生成される。ここで、上記突然変異パラメータとしては、突然変異の発生確率 $q_+$ 、位置の確率 $q_1$ 、幅確率 $q_\phi$ の他、数の確率 $q_n$ 等が存在する。ステップS9で、突然変異手段8によって、上記突然変異パラメータに基づいて突然変異処理が行われる。その際に、二重化(多重化)されたコンテンツ側のコンテンツDNAとコピー装置4側のコンテンツDNAとの何れのコンテンツDNAに突然変異を発生させるかも決定される。

【0074】ステップS10で、上記暗号化手段9によって、コンテンツDNAが暗号化される。ここで、本実施形態においては、暗号化方式については特に制限はない。尚、図6に示すフローチャートにおいては、暗号化処理は突然変異後に1回だけ実行するようになっている。しかしながら、この説明においては、参照したコンテンツあるいはコピーの主体の「D(図3(a))、交叉

処理を行う際のコンテンツDNA。交叉処理を行った後のコンテンツDNA。突然変異処理を行った後のコンテンツDNA等に対して、1回または複数回実行することが可能になっている。

【0075】ステップS11で、上記電子透かし情報生成手段10によって、上記ステップS10において暗号化されたコンテンツDNAから電子透かし情報が生成される。この場合、電子透かし情報生成手段10を、後に述べるようにコンテンツの種類に応じて異なる透かしデータを適宜可能に生成することも可能である。ステップS12で、コピー制御手段2によって、コンテンツ流通管理情報記録手段3からのコピー履歴情報を兼ねる電子透かし情報(コンテンツDNA)を登録する記録処理が実行される。尚、ここで言う「コンテンツDNAの記録」とは、コピー元のコンテンツに書き込んでコピー装置4に送達する処理、記録手段1に記録されているコピー元のコンテンツに追加して書き込む処理、および、記録手段1に直接保存する処理である。

【0076】ステップS13で、上記ステップS3においてコピー部と判別された場合には、コピー実行が阻止される。

【0077】尚、上記コンテンツ流通管理情報記録処理動作のフローチャートにおいては、コピー可否の判定には、選択手段5による情報の一意化、融合手段6による融合処理、交叉手段7による交叉処理、突然変異手段8による突然変異処理の後に実行された後に、暗号化手段9によって暗号化が行われるようになっている。しかしながら、本実施の形態におけるコンテンツ流通管理情報記録処理動作はこれに限定されるものではなく、情報の一意化→暗号化、情報の一意化→融合処理→暗号化、情報の一意化→融合処理→交叉処理→暗号化、情報の一意化→融合処理→突然変異処理→暗号化等の種々のコンテンツ流通管理情報記録処理が可能である。

【0078】図7は、コンテンツを管理するために各コンテンツに付加されたヘッダ情報の一例を示す。このヘッダ情報は、付加されているコンテンツと共に記録手段1に記録されている。

【0079】図7において、【コンテンツの種類m】から始まって【保護期間n】に終わるレコードは、著作物の著作権情報を保持したものである。このうち、レコード50, 61は二次的著作物に関する著作権情報である。また、レコード41, 47, 53は、【コンテンツIDm】を表す情報である。このレコードには、コンテンツを識別するためのID番号が登録される。尚、上記ID番号は、当該メディアの番号とコンテンツIDとのシリアル化並び組み合わせた識別子であってもよい。その場合、コンテンツIDは並び順で決まることができるため省略されることもあり得る。

【0080】レコード42, 48, 54は、【コンテンツの種類(コンテンツタイプ)m】を表している。本実施の形態においては著作権で保護されるコンテンツを対象としており、例えば、コンテンツの種類には、小説、脚本、論文、講演およびその他の言語的著作物、音楽の著作物、舞踏または演劇の著作物、絵画、版画、彫刻およびその他の美術の著作物、建築の著作物、地図、学術的な性質を有する図画、図表、模型およびその他の図解的著作物、映画の著作物、写真の著作物、プログラムの著作物等がある。これらのコンテンツの種類は、コンテンツが生出された国や消費される国によって対象が少し異なる場合があるが、発明の要旨には変わりはない。

【0081】レコード43~45、レコード49~51、レコード55~57は、それぞれコンテンツの種類4, 2, 48, 54に対応した「著作権」を表している。著作権は、共同著作権の有無によってその数が決まる。例えば、原著作者の共同著作権がp人、二次的著作物60の共同著作権がq人、二次的著作物61の共同著作権がr人〜57はr人である。著作権者のレコード43~45, 49~51, 55~57中に登録される情報は著作権者を特定できるものであり、例えば、氏名若しくは名称(実名)またはその別号、漢名、別称およびその他の名に代えて用いられるもの(愛称)がある。または、これらと住所や職業等の他の属性との組み合わせ、或はこれらの著作権者を特定することができるIDコードであってもよい。尚、著作権はコンテンツの種類によっても変化する。例えば、コンテンツの種類が映画である場合、著作権としては、制作、監督、演出、撮影、美術、音楽等を担当してその映画に関する著作物の全体的形成に創作的に寄与したものが帰属する。また、コンテンツの種類が音楽である場合には作曲家、作詞家、編曲家、演奏家および歌手等が著作権者に相当し、小説である場合には作家、脚本家および文庫家等が著作権者に相当する。

【0082】レコード46, 52, 58は、コンテンツID41, 47, 53に対応した【コンテンツ保護期間m】を表す情報であり、延命は有効期間の最終日が登録されている。

【0083】ここで、上記コンテンツIDとコンテンツの種類とによって、コンテンツの単位や構造が異なる。例えば、コンテンツの種類が言語的著作物(以後、「ドキュメント」若しくは文書と言う場合がある)の場合は、文書全体を表すコンテンツIDの他に、目次、表、目、ページ、索引、図表、行、文字等の構造がある。尚、図6に示すコンテンツ流通管理情報記録処理動作における上記ステップS1でのコピー要求は、上記構造を単位として1単位または複数の単位に対して行われる。したがって、コピー装置4からのコピー要求としては、コンテンツ全体へのコピー要求の他に、上記単位を指定することによって、例えばコンテンツIDが「a」であるコンテンツ中における「第1章の第5段落から第8段落まで」の如く領域

コピーの要求も可能になる。

【0084】次に、図8に示すコンテンツ流通管理情報記録処理動作における上記ステップS11において、上記電子透かし情報生成可能10によって実行される電子透かし情報生成処理について詳細に説明する。図8は、電子透かし情報生成処理動作のフローチャートである。図8のフローチャートにおける上記ステップS10において、符号化処理が終了すると電子透かし情報生成処理動作がスタートする。

【0085】ステップS21で、上記コピー装置4から要求されるコピーのコピー対象が判別される。ステップS22で、コピー装置4から要求されるコピーの範囲が参照される。ステップS23で、コピー装置4から要求されるコピー対象のコンテンツタイプ(コンテンツの種類)が参照される。これらの参照は、記憶手段1に格納されている各コンテンツのヘッダ情報に対して行われる。そして、上記参照の結果、具体的な情報(内容)が得られる。

【0086】ステップS24で、上記ステップS21～ステップS23における参照結果、コンテンツの種類は「イメージ」であるか否かが判別される。その結果、イメージであればステップS25に進み、そうでなければステップS28に進む。ステップS25で、コンテンツの種類は「静止画」であるか否かが判別される。その結果、静止画であればステップS26に進み、そうでなければステップS27に進む。ステップS26で、静止画透かし方法が選択される。そうした後に、ステップS23に進む。ここで、静止画透かし方法には、画素パターン法、組織的ディザ法、画素置換法等が存在する。そして、イメージデータに画素情報がある場合は、画素置換、画素置換利用、量子化画素利用、画素置換利用、統計置換利用等の各種の透かし方法が知られている。本実施の形態においては、静止画透かし方法については特に特定はしない。ステップS27で、動画透かし方法が選択される。そうした後に、ステップS33に進む。ここで、「動画透かし方法」には、MPEG(ムービング・ピクチャー・エキスパート・グループ)1、MPEG2、MPEG4等の規格に応じて透かし方法が知られている。本実施の形態においては、動画透かし方法については特に特定はしない。

【0087】ステップS28で、コンテンツの種類は「音声」であるか否かが判別される。その結果、音声であればステップS29に進み、そうでなければステップS30に進む。ステップS29で、音声透かし方法が選択される。そうした後に、ステップS33に進む。ここで、「音声透かし方法」には、アナログ形式、音声量子化、音声スキャン、予測符号化、ランレングス、ベクトル量子化、音源パルス等の透かし方法が知られている。本実施の形態においては、音声透かし方法については特に特定はしない。

【0088】ステップS30で、コンテンツの種類は「文書」であるか否かが判別される。その結果、文書であればステップS31に進み、そうでなければステップS32に進

進む。ステップS31で、文書透かし方法が選択される。そうした後に、ステップS33に進む。ここで、「文書透かし方法」には、欧文と和文かで透かし生成方法を定める方法が知られている。ステップS32で、その他の「コンテンツの種類」に付いた透かし方法が選択される。上述のごとく、本実施の形態においては電子透かし方法については問題にせず、コンテンツの種類に応じて電子透かし方法が少なくとも一つ選択できればよい。

【0089】ステップS33で、上述のようにして選択された透かし方法によって電子透かし情報が生成可能か否かが判別される。その結果、生成可能であればステップS36に進み、生成不可能であればステップS34に進む。ここで、本実施の形態においてコピー対象にある各々の電子透かし情報は、法定長を有するコンテンツDNAである。したがって、コピー単位(つまり、コピー対象の範囲)がコンテンツDNAに比べて充分に小さい場合には、得られた電子透かし情報を書き込むことができないために電子透かし情報の生成は不可能であると判定するのである。ステップS34で、透かし情報書き込み領域は最大か否かが判別される。その結果、最大であれば上記コンテンツ流通管理情報記録処理動作における上記ステップS13にリターンして、当該コピーが返却される。一方、最大でなければステップS35に進む。ここで、上記透かし情報書き込み領域の最大は、コピー対象であるコンテンツ1Dのコンテンツ全体である。

【0090】ステップS35で、上記電子透かし情報書き込み領域が現在の領域よりも1ランク上の(1単位大きい)領域に拡大される。ここで、電子透かし情報書き込み領域の初期値は、上記ステップS22における参照の結果得られたコピー範囲(単位)である。そうした後、上記ステップS23に戻って、再度電子透かし方法の選択が行われる。そして、上記ステップS33において電子透かし情報が生成可能と判定されると、ステップS36に進む。

【0091】ステップS36で、現在の透かし情報書き込み領域に基づいて、電子透かし書き込み領域が決定される。ステップS37で、上記選択された電子透かし方法によって、コンテンツDNAの電子透かし情報が生成される。そうした後に、上記コンテンツ流通管理情報記録処理動作における上記ステップS12にリターンして、記録処理が実行される。その結果、上記ステップS37において生成されたコンテンツDNAの電子透かし情報が、コピー元およびコピー先の両コンテンツにおける上記ステップS36において決定された電子透かし書き込み領域に書き込まれる。そして、このコンテンツDNA(電子透かし情報)が書き込まれたコピー先のコンテンツがコピー装置4に返送される。

【0092】次に、上述のようにしてコンテンツに書き込まれたコンテンツDNA(電子透かし情報)に基づいて、コピー装置を通過する処理について説明する。図9は、一つのコンテンツが複数コピーされた場合における

コンテンツDNAの差違を示す。図9における65は、コンテンツにおけるオリジナル(第1世代)のコンテンツDNAである。同様に、66はコピー装置AにおけるオリジナルのコンテンツDNAであり、67はコピー装置BにおけるオリジナルのコンテンツDNAであり、68はコピー装置CにおけるオリジナルのコンテンツDNAである。

【0093】コンテンツ内のオリジナルコンテンツDNAとコピー装置AのオリジナルコンテンツDNAとが融合手段6によって融合されると、第2世代のコンテンツDNA 69が生成される。同様に、65との由来のオリジナルコンテンツDNAが対を成していることが分かる。このコンテンツDNA対に対して交叉手段7によって交叉が行われるとコンテンツDNA 70が生成される。尚、上記交叉の対象となる領域の中には上記複製異常によって一部の領域が変更されたものも含まれるが、以後においては交叉に含めて説明する。

【0094】次に、上記交叉後の第2世代コンテンツDNA 70とコピー装置BのオリジナルコンテンツDNA 67との間で融合が行われると、第3世代のコンテンツDNA 71が生成される。そして、コンテンツDNA 71のコンテンツDNA対に対して交叉が行われるとコンテンツDNA 72が生成される。同様に、交叉後の第3世代コンテンツDNA 72とコピー装置CのオリジナルコンテンツDNA 68との間で融合が行われると、第4世代のコンテンツDNA 73が生成される。そして、コンテンツDNA 73のコンテンツDNA対に対して交叉が行われるとコンテンツDNA 74が生成される。

【0095】本実施の形態における「コピー履歴を抽出する」とは、交叉後の第4世代のコンテンツDNA 74が与えられて、交叉前の第4世代のコンテンツDNA 73、交叉前の第3世代のコンテンツDNA 72、71、交叉前の第2世代のコンテンツDNA 70、69とコンテンツDNAの差違を辿りながら、コピーに關与したコピー装置A～CのオリジナルコンテンツDNA 66～68を明らかにすることである。

【0096】図10は、上記コピー制御手段2の制御の下に、コンテンツ差違管理情報記録手段3によって実行されるコピー履歴追跡処理動作のフローチャートである。以下、図10に従って、コピー履歴追跡処理について説明する。尚、その際における追跡の元となるコンテンツDNAは、図9におけるコピー順序で生成されたものとする。

【0097】ステップS41で、上記コピー制御手段2によって、追跡の対象となるコンテンツあるいは記録手段1に書き込まれて蓄積されているコンテンツDNAの中から最新のコンテンツDNA 74が抽出される。ここで、最新のコンテンツDNAの隣には、対を成すコンテンツDNAの双方が一層複雑なコンテンツDNAを選択すればよい。尚、最新のコンテンツDNAの抽出を高度

化するためには、コンテンツにコンテンツDNAを蓄積する際に、コピーの順とコンテンツDNAの書き込みアドレスとのインデックスを作成しておけばよい。

【0098】ステップS42で、上記コンテンツ差違管理情報記録手段3における番号手段11によって、上記ステップS41において抽出された最新のコンテンツDNA 74が複写化される。ステップS43で、上記コピー制御手段2の番号手段12によって、上記ステップS42において複写化された最新のコンテンツDNA 74と各コピー装置A～CのオリジナルコンテンツDNA 66～68との差分が求められる。尚、各コピー装置A～CのオリジナルコンテンツDNA 66～68は、過去にコピーが実行された際に記録手段1に格納されて保存されている。ステップS44で、最小の差分を呈するオリジナルコンテンツDNAが求められる。本例の場合には、コピー装置CのオリジナルコンテンツDNA 68が最新コンテンツDNA 74における一方(図9において下側)のコンテンツDNA 74bと比較された場合に、最小差分となる。

【0099】ステップS45で、上記最小の差分を呈するオリジナルコンテンツDNA 68のコピー装置Cが、コピー主体として選択される。ステップS46で、上記選択されたコピー主体のオリジナルコンテンツDNA 68と上記最小差分を呈する最新コンテンツDNA 74の上記一方のコンテンツDNA 74bとの差分が求められる。その結果、本例の場合には、下側のコンテンツDNA 74bにおける第1制御領域75と第2制御領域76とが抽出される。

【0100】ステップS47で、上記ステップS46において抽出された領域75、76の情報を、対の(上側の)コンテンツDNA 74aにおける対応する領域77の情報と入れ替える修正処理が行われる。その結果、最新コンテンツDNAである交叉後のコンテンツDNA 74が交叉前のコンテンツDNA 73に置かれる。その場合、得られた交叉前のコンテンツDNA 73における下側のコンテンツDNA 73bとコピー主体のオリジナルコンテンツDNA 68とのマッチ度が最大になるようにビット反転し、突然変異で生じたデータ変形をも修正する。ステップS48で、上記ステップS47における修正の結果得られた交叉前のコンテンツDNA 73bが、コピー主体のオリジナルコンテンツDNA 68に一致するか否かが判別される。その結果、一致すればステップS49に進み、一致しなければ、上記ステップS47に居って上記突然変異の修正等が繰返される。

【0101】ステップS48で、上述のようにして修正の結果得られた交叉前のコンテンツDNA 73が、当世代のコンテンツDNAとして決定される。ステップS49で、上記決定された当世代のコンテンツDNA 73における下側のコンテンツDNA 73bと同じ内容のオリジナルコンテンツDNA 68を有するコピー装置Cが、当世代のコンテンツDNA 73の生成に關与したコピー装

物であると特定される。ステップS51で、前世代のコテンツDNA73における上側のコテンツDNA73aから、前世代のコテンツに属するコテンツDNAが求められる。

【0102】ステップS52で、上記ステップS51において求められた前世代のコテンツDNA73aに属するコテンツDNA73aは、オリジナルコテンツDNAであるか否かが判別される。その結果、オリジナルコテンツDNAであればコピー履歴追跡処理動作を終了する。一方、オリジナルコテンツDNAでなければステップS53に進む。

【0103】ステップS53で、上記ステップS51において求められた前世代のコテンツDNA73aを有する前世代コテンツDNA73が、当該コテンツに格納されている全コテンツDNAから、あるいは、上記インデックスから検索される。ステップS54で、上記ステップS53における検索の結果、該当する前世代コテンツDNAが当該コテンツのDNA情報に存在するか否かが判断される。その結果、存在場合には上記ステップS43に遷って更に前世代に属する履歴追跡処理に移行する。一方、無い場合にはステップS55に進む。ここで、更に前世代に属する履歴追跡処理に移行する場合には、上記ステップS43および上記ステップS48における「最新のコテンツDNA74」には「コテンツDNA72」を当て換える。そして、上記ステップS52において、前世代のコテンツに属するコテンツDNAはオリジナルコテンツDNAであると判断されると、コピー履歴追跡処理動作を終了する。ステップS55で、エラー表示が行われた後コピー履歴追跡処理動作を終了する。

【0104】次に、上記図6に示すコテンツ流通管理情報記録処理動作における上記ステップS2及びステップS3において実行されるコピー可否の判定処理について、詳細に説明する。図11は、コピーの制限情報を記録する際のデータ構造を示す。このコピー制限情報は、コテンツまたは記憶手段1における通常のコピー命令（つまり、論理命令）では読み出せない特定領域に書き込まれている。

【0105】図11において、レコード81、82、89は、コピー対象コテンツのID番号を記録するレコードである。このレコード81、82、89の内容は、図7に示すヘッダ情報におけるコテンツID41、42、53の内容と同じである。レコード83、84、85、86、91は、コテンツのコピーが許可されたコピー装置のIDを記録するレコードである。レコード83、85、87は、コテンツID1に属するコテンツに対する各コピー装置によるコピー制限回数を記録しておくレコードである。同様に、レコード88には、コテンツIDが「m」のコテンツに対するコピー装置IDが「x」のコピー装置によるコピー制限回数が記録されている。

【0106】すなわち、コピー情報93は、コテンツIDが「1」であるコテンツに属するコピー情報である。同様に、コピー情報94、95は、コテンツIDが「2」、「m」であるコテンツに属するコピー情報である。尚、上述のコピー情報は、コテンツDNAを生成する際に用いられる暗号化アルゴリズムによって暗号化されているものとする。

【0107】図12は、コピー可否判定処理動作のフローチャートである。上記図6に示すコテンツ流通管理情報記録処理動作における上記ステップS3においてコピー要求があると判断されると、上記コピー可否判定処理動作がスタートする。

【0108】ステップS61で、コピー要求を行ったコピー装置を特定する歩みコピー装置の特定が実行される。尚、要求コピー装置の特定は、コピー対象のコテンツあるいは記憶手段1における上記特定領域に書き込まれているコピー制限情報（図11）を参照することによって行われる。また、この処理は、通常のコピー命令の前に実行される。ステップS62で、要求コピー装置の特定が成功したか否かが判断される。その結果、成功した場合には、コピー要求を出したコピー装置はコピー許可対象装置であると認定されてステップS63に進む。一方、失敗した場合には、不正コピーの可能性が大であるとして、上記コテンツ流通管理情報記録処理動作における上記ステップS13にリターンする。

【0109】ステップS63で、コピー対象と上記コピー許可対象装置であるコピー装置のIDとに基づいて、当該コピー対象内に格納されているコテンツDNAが参照される。ステップS64で、上記コテンツDNAの参照結果に基づいて、当該コピー要求を出しているコピー装置が、当該コピー対象を過去に何回コピーしたかを検索する過程履歴追跡処理が実行される。その場合における検索の方法は、図10に示すコピー履歴追跡処理動作に準ずる。

【0110】ステップS65で、上記コピー制限情報（図11）の内容が参照される。ステップS66で、上記参照の結果に基づいて、要求を出したコピー装置およびコピー対象に関わるコピー制限回数と上記過去のコピー履歴とが比較され、今回の要求によるコピー回数がコピー制限回数以下であるか否かが判断される。その結果、以下であれば、上記コテンツ流通管理情報記録処理動作における上記ステップS4にリターンして、新たなコテンツDNAの生成が開始される。一方、そうでなければ、上記コテンツ流通管理情報記録処理動作における上記ステップS13にリターンする。

【0111】上述のように、本実施の形態においては、コテンツおよびコテンツDNAを記録・復元する記憶手段1と、上記コテンツのコピー可否の判断やコピー履歴の追跡やコピー実行を制御するコピー制御手段2と、コテンツおよびコピー装置4のコテンツDNA

に基づいて新たなコンテンツDNAを生成してコピーされたコンテンツに書き込んで記録するコンテンツ流通管理情報記録手段3を備えている。

【0112】そして、上記コンテンツ流通管理情報記録手段3によってコンテンツDNAを生成する場合には、選択手段5によって二重化されているコンテンツ側のコンテンツDNAの一つを選択し、融合手段6によって上記選択されたコンテンツ側のコンテンツDNAとコピー装置4側のオリジナルコンテンツDNAとを組み合わせて二重化して新たなコンテンツDNAを生成する。そして更に、上記コンテンツ流通管理情報記録手段3の交叉手段7によって、二重化された新たなコンテンツDNAにおけるコンテンツDNA対に対して交叉を行う。また、必要に応じて突然変異手段8によって突然変異を行う。

【0113】一方、各コンテンツあるいは記録手段1には、通常のコピー命令（複製命令）では読み出せない特定領域に、コピー許可対象のコピー装置のIDとそのコピー装置によるコピー制限回数を含むコピー制限情報が書き込まれている。

【0114】上記コピー制御手段9は、コピー装置4からコピー要求を受けると、上記コピー制限情報を参照し、要求コピー装置4がコピー許可対象装置でない場合にはコピー拒否するようにしている。したがって、本実施の形態によれば、不正コピーの防止を行うことができるのである。

【0115】一方、コピー許可対象装置である場合には、コンテンツ流通管理情報記録手段3に対してコピー履歴の追跡を指示する。そうすると、コンテンツ流通管理情報記録手段3のコピー履歴追跡手段12によって、記録手段1に蓄積されているコンテンツDNAの履歴と過去にコピーを行なったコピー装置のオリジナルコンテンツDNAとの比較を行いながら、当該コンテンツのオリジナルコンテンツDNAに通り付くまで上記融合、交叉および突然変異の逆の手順を行う。その結果、当該コンテンツのオリジナルコンテンツDNAが最新のコンテンツDNAに変化するまでに交叉されたコピー装置側のオリジナルコンテンツDNAを抽出できるのである。

【0116】したがって、こうして得られた過去にコピーを行ったコピー装置およびコピー回数と、上記コピー履歴情報の内容と、今要求を出しているコピー装置のIDとに基づいて、今出されているコピー要求を受け付けるか拒否するかを判定できる。すなわち、本実施の形態によれば、例えば上記不正コピー防止策が破られたとしても、無断に不正コピーされることを防止できるのである。

【0117】さらに、上記記録手段1に格納されているコンテンツが不正にコピーされて市場に出回っている場合には、不正コピーコンテンツに書き込み蓄積されているコンテンツDNAの履歴に基づいて、上述のコピー版

歴の追跡を行うことによって不正コピーに向わるコピー装置を解明できる。したがって、不正コピーの発生源を突き止めることができるのである。

【0118】また、本実施の形態においては、コピー時に生成されたコンテンツDNAは、例えばコンテンツがドキュメントや文書の場合は目次、章、節、ページ、段落あるいは行等の各コンテンツの構成に関連した単位で書き込むことが可能である。したがって、各コンテンツに比した単位でコンテンツDNAを埋め込むことができ、コンテンツの部分的な不正コピーに対しても耐性が高くなる。

【0119】また、本実施の形態においては、上述のように、コンテンツをコピーする際に必要なコンテンツDNAには交叉処理や突然変異処理が行われている。さらに、コンテンツ流通管理情報記録手段3の暗号化手段9および電子透かし情報生成手段10によって、上述のようにして生成されたコンテンツDNAを暗号化および電子透かし情報化して情報の複製・転送を行っている。したがって、上記ICD等の機器を使って不正にコンテンツを読み出してもコンテンツDNAの内容を解読したり改ざんすることは不可能である。さらに、上記コピー制限情報は、コンテンツあるいは記録手段1の通常のコピー命令（複製命令）では読み出せない特定領域に書き込まれている。したがって、このコピー制限情報の存在そのものが隠れかきになることは無い。

【0120】また、本実施の形態においては、上記コンテンツDNAの情報量は選択手段5および融合手段6の作用によって一定に保たれる。したがって、コピー操作を繰り返しても履歴情報量（コンテンツDNAの情報量）は増えることがない。

【0121】ところで、上記実施の形態におけるコピー制御手段2、コンテンツ流通管理情報記録手段3、選択手段5、融合手段6、交叉手段7、突然変異手段8、暗号化手段9、電子透かし情報生成手段10、復号化手段11およびコピー履歴追跡手段12としての機能は、プログラム記憶媒体に記録されたコンテンツ流通管理情報記録処理プログラムや電子透かし情報生成・記録処理プログラムやコピー履歴追跡処理プログラムやコピー可否判定処理プログラムによって実現される。

【0122】上記実施の形態における上記プログラム記憶媒体は、上記記録手段1とは別体に設けられたROM（リード・オンリ・メモリ：読み専用）であるプログラムノディアである。あるいは、外部補助記憶装置（図示せず）に装着されて読み出されるプログラムメディアであってもよい。尚、何れの場合においても、上記プログラムメディアから上記各処理プログラムを読み出すプログラム読み出し手段は、上記プログラムメディアに直接アクセスして読み出す構成を有していてもよいし、RAM（図示せず）に設けられたプログラム記憶エリアにダウンロードし、上記プログラム記憶エリアにアクセスして読み

出す構成を有していてもよい。例、上記プログラムメディアから上記RAMのプログラム記憶エリアにダウンロードするためのダウンロードプログラムは、予め本体装置に格納されているものとする。

【0123】ここで、上記プログラムメディアとは、本装置と分離可能に構成され、磁気テープやカセットテープ等のテープ系、FD、フロッピーディスク等の磁気ディスクやCD(コンパクトディスク)・ROM、MOD/MD(ミニディスク)、DVD等の光ディスクのディスク系、IC(集積回路)カードやメモリカード等のカード系、マスクROM、EPROM(紫外線消去型ROM)、EEPROM(電気的消去型ROM)、フラッシュROM等の半導体メモリ系を含めた、固定的にプログラムを記憶する媒体である。

【0124】また、上記装置の接続におけるコンテンツ流通管理装置は、モデムを備えてインターネットを含む通信ネットワークと接続可能な構成を有している場合には、上記プログラムメディアは、通信ネットワークからのダウンロード等によって自動的にプログラムを記憶する媒体であっても差し支えない。なお、その場合における上記通信ネットワークからダウンロードするためのダウンロードプログラムは、予め本体装置に格納されているものとする。あるいは、事前記憶媒体からインストールされるものとする。

【0125】尚、上記記憶媒体に記録されるものはプログラムの系に限定されるものではなく、データも記録することが可能である。

【0126】

【効果】以上より明らかなように、第1の発明のコンテンツ流通管理装置は、コンテンツ流通管理情報記録手段によって、コンテンツの属性を表す情報およびコピー主体の属性を表す情報とを多量化して格納できるコンテンツDNAを生成して、コピー元およびコピー先の両コンテンツのコピー対象領域に記録するので、コピーされたコンテンツのコピー対象領域にはコピー履歴情報が記録されることになる。したがって、不正にコピーされたコンテンツあるいはそのコピー対象領域に記録されているコンテンツDNAに基づいて、コピーの履歴を追跡してコピー主体を特定することが可能となる。すなわち、この発明によれば、不正コピーの発生源を突き止めることができる。

【0127】また、上記第1の発明は、上記コンテンツ流通管理情報記録手段によって上記コンテンツDNAを多量化して記録すれば、上記コンテンツの属性を表す情報と上記コピー主体の属性を表す情報とを多量化して、1つのコンテンツDNAとすることが可能となる。したがって、上記コンテンツDNAを解析することによって、上記コンテンツとコピー主体との関係を解明できる。

【0128】また、上記第1の発明は、上記コンテンツ

流通管理情報記録手段に、コピー実行の際に、上記コンテンツに多量化されて記録されているコンテンツDNAから一意の情報を選択する選択手段と、上記選択された一意の情報をコピー主体の属性を表す情報とに基づいて多量化された新たなコンテンツDNAを生成する融合手段を備えれば、上記コンテンツの属性を表す情報とコピー主体の属性を表す情報とを多量化して1つのコンテンツDNAを生成できる。したがって、上記コンテンツDNAを解析することによって、両者のコンテンツが何れのコピー主体によってコピーされたかを容易に解明できる。

【0129】その際に、上記新たに生成されたコンテンツDNAは、上記コンテンツのコピー対象領域に記録されている元のコンテンツDNAと同じ情報量を有している。したがって、コピー操作を繰り返しても上記情報量を一定に保つことができ、コピーの履歴情報が増えることを防止できる。

【0130】また、上記第1の発明は、交叉手段によって、上記融合手段で生成されたコンテンツDNAを構成する系を複数情報間で情報の一部を交換すれば、現在までコピーに拘わったコピー主体の属性を表す情報が格納されたコンテンツDNAを容易に生成できる。

【0131】また、上記第1の発明における上記交叉手段を、予め設定された交叉関数に基づいて、上記融合手段における交叉の位置、交叉の幅および交叉の発生頻度を制御するようにすれば、現在までコピーに拘わった全てのコピー主体の属性を表す情報が失われることなく格納され、且つ、内容が増大されているコンテンツDNAを生成することができる。

【0132】また、上記第1の発明は、突然変異手段によって、上記生成されたコンテンツDNAの一部を変異すれば、上記コンテンツDNAの内容を攪乱させて、上記コンテンツDNAの内容が外部に漏れることを防止できる。

【0133】また、上記第1の発明における上記突然変異手段を、予め設定された突然変異関数に基づいて、上記変異の位置、変異の幅及び変異の発生頻度を制御するようにすれば、上記コンテンツDNAの内容をより効果的に攪乱することができる。

【0134】また、上記第1の発明は、上記コンテンツのコピー対象領域を当該コンテンツの構成に関連する単位とすれば、コンテンツの構成に関連する単位で上記コンテンツDNAを記録できる。したがって、コンテンツの部分的な不正コピーに対する耐性を高くできる。

【0135】また、上記第1の発明は、暗号化手段によって、上記生成されたコンテンツDNAを暗号化すれば、上記コンテンツDNAの内容を攪乱・隠蔽することができる。したがって、上記コンテンツDNAの内容が外部に漏れることを効果的に防止できる。

【0136】また、上記第1の発明は、電子透かし情報



生成手段によって、上記暗号化されたコンテンツDNAに基づいて電子透かし情報を生成すれば、上記コンテンツDNAの内容をより完全に複製・鑑別できる。したがって、上記コンテンツDNAの内容が外部に漏れることを所定の範囲に防止できる。

【0137】また、上記第1の発明は、コピー履歴追跡手段によって、上記コンテンツに記録されている上記コンテンツDNAに基づいてコピーの履歴を追跡してコピー主体を特定するようにすれば、不正コピーされたコンテンツに閉するコピーの履歴を追跡して、不正コピーの発生源を容易に突き止めることができる。

【0138】また、上記第1の発明は、復号手段によって復号化されたコンテンツDNAに基づいて、コピー履歴追跡手段によって、コピーの履歴を追跡してコピー主体を特定するようにすれば、不正にコピーされたコンテンツに記録されているコンテンツDNAが暗号化されていても、コピーの履歴を追跡してコピー主体を特定することができる。

【0139】また、上記第1の発明は、コピーが許可されたコピー主体の情報を含むコピー制御情報を上記記憶手段における記憶命令では読み出せない特定領域に記憶し、上記コピー制御手段によって、要求コピー主体が上記コピー制御情報に格納されているコピー主体である場合にのみ上記コンテンツ流通管理情報記録手段に上記コンテンツDNAの生成を指示するようにすれば、コピー許可対象のコピー主体に対してのみコピーを許可して、コピー許可対象ではないコピー主体からの不正コピーを防止できる。さらに、上記コピー制御情報は、複製命令では読み出せない特定領域に記憶されているので、通常のコピー命令で読み出されて改ざんされることを防止できる。

【0140】また、上記第1の発明は、上記コピー制御手段を、上記要求コピー主体が上記コピー制御情報に登録されていないコピー主体である場合にはコピーの実行を禁止するかあるいはコピー禁止メッセージを表示するようにすれば、コピー許可対象ではないコピー主体による不正コピーを防止できる。

【0141】また、第2の発明のプログラム記録媒体は、コンピュータを、記憶手段における記憶命令では読み出せない特定領域に上記コピー制御情報を格納する情報記録手段と、上記コンテンツDNAを生成するコンテンツ流通管理情報生成手段と、上記交叉を行う交叉手段と、上記突然変異を行う突然変異手段と、上記暗号化を行う暗号化手段と、上記電子透かし情報を生成して記録する電子透かし情報生成手段と、上記コンテンツDNAを復号化する復号手段と、コピーの履歴を追跡してコピー主体を特定するコピー履歴追跡手段と、上記コピー制御情報に登録されているコピー主体からの要求である場合にのみコピーを実行するコピー制御手段として機能させるコンテンツ流通管理情報プログラムおよびコピー

履歴追跡プログラムが記録されているので、不正にコピーされたコンテンツに記録されているコンテンツDNAに基づいて、不正コピーの発生源を容易に突き止めることができる。

【0142】さらに、上記コンテンツDNAの内容を混乱・隠蔽して、上記コンテンツDNAの内容が外部に漏れることを効果的に防止できる。また、コピー許可対象ではないコピー主体による不正コピーを防止できる。

【図面の簡単な説明】

【図1】 この発明のコンテンツ流通管理装置におけるブロック図である。

【図2】 図1におけるコンテンツ流通管理情報記録手段の内部構造を示すブロック図である。

【図3】 コンテンツDNAおよびその暗号化の一例を示す図である。

【図4】 コンテンツDNAに対する融合、交叉および突然変異の説明図である。

【図5】 コンテンツDNAに対して交叉が行われた状態を表す概念図である。

【図6】 コンテンツ流通管理情報記録処理動作のフローチャートである。

【図7】 各コンテンツに行加されたハッシュ値のデータ構造を示す図である。

【図8】 電子透かし情報生成処理動作のフローチャートである。

【図9】 要求コピーが行われた場合におけるコンテンツDNAの変遷を示す図である。

【図10】 コピー履歴追跡処理動作のフローチャートである。

【図11】 コピー制御情報のデータ構造を示す図である。

【図12】 コピー許可判定処理動作のフローチャートである。

【符号の説明】

1…記憶手段、 2…コピー制御手段、 3…コンテンツ流通管理情報記録手段、 4…コピー装置、

5…選択手段、 6…融合手段、

7…交叉手段、 8…突然変異手段、

9…暗号化手段、 10…電子透かし情報生成手段、

11…復号手段、 12…コピー履歴追跡手段、 13…原著物に関する著作権情報、

14、15…二次的著作物に関する著作権情報、 16、17、18…コンテンツID、 19、20、21…コンテンツの領域、

22～24、25、26…コンテンツ保護期間、 27…コンテンツのオリジナルコンテンツDNA、

28、29、30…コピー装置のオリジナルのコンテンツDNA、 31…交叉前の第2世代コンテンツDNA、

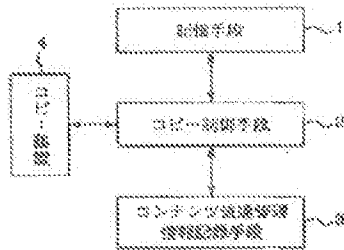
32…交叉後の第2世代コンテンツDNA、 33…交叉前の第3世代コンテンツDNA、

34…交叉後の第3世代コンテンツDNA

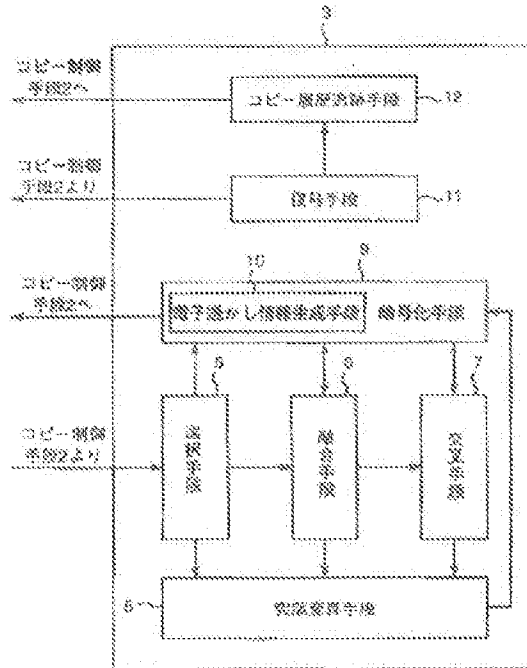
A、アタカ変異前の第4世代コンプレックスDNA、74→  
変異後の第4世代コンプレックスDNA、81、88、89→

コンプレックス1D、82、83、86、90、ワットコピー表  
置1D、82、85、87、92→コピー制御回路。

【図1】



【図2】



【図3】

(a) 50387-881-8858888-84376

(b)

h1wDcPKU3WwVVCx2A69Z2hce/pDskR35w9Q4a31UPdKK  
3Dm5EGT5oAq1D6g/s  
FLV2Bt1AxwD9Q884c1n2j9w9Qw88U2Z1aC2j9W9g8h8e  
8H2F51-C5e36s  
UpRdZ5LHoxN6G21k+5owF3NajAoc3C5BEdUmLE2aC1wH6  
QVx5-12F1Ioc7C68K7A  
AA8868h9wvca6Lg6XUg8888SVa2c2j9w9Q4a31UPdKK  
23w9FD3j9cNuc71a  
Qw884c88gK1H2462r  
wshT

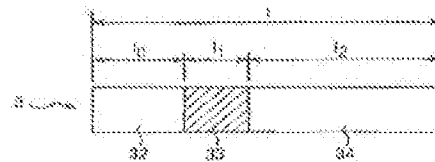
(c)

h1wDcPKU3WwVVCx2A69Z2hce/pDskR35w9Q4a31UPdKK

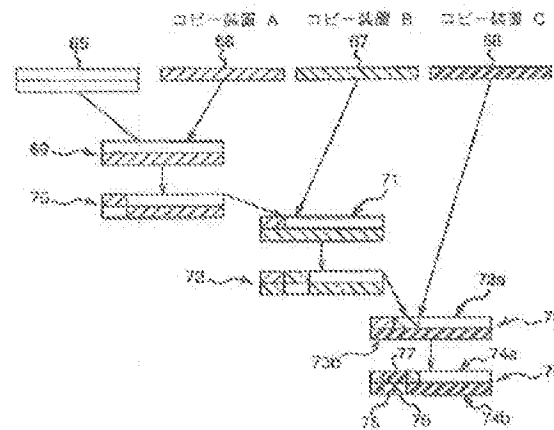
(d)

h1wDcPKU3WwVVCx2A69Z2hce/pDskR35w9Q4a31UPdKK  
h1wDcPKU3WwVVCx2A69Z2hce/pDskR35w9Q4a31UPdKK

【図5】

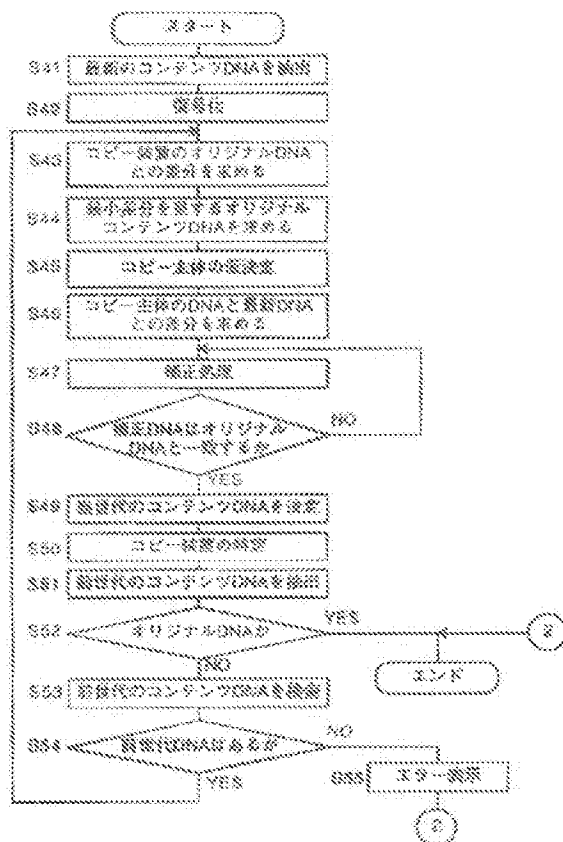


【図9】

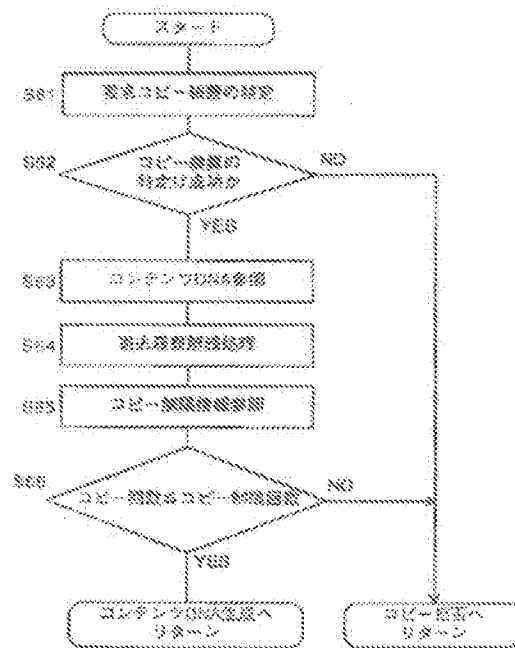




184 01



【図12】



フロントページの続き

Fターム(参考) 5B017 AA06 SA06 EA07 BB03 CA07  
 CA08 CA09 CA11 CA14 CA16  
 5B044 AB01 DE06 GK12 GK17 HL02  
 HL03  
 5B110 BC14 CA06 DA12 DB17 DE05  
 DE04 DE06  
 5J104 AA14 BA05 FA14  
 5A001 BB06 EE03 LL03



# PATENT ABSTRACTS OF JAPAN

(11) Publication number : 2001-023297

(43) Date of publication of application : 26.01.2001

(S) Int. Cl.

G31B 20/10

G06F 12/14

G09C 5/00

G11B 27/00

(21)Application number : 11-189023

(7)Applicant : SHARP CORP

(22) Date of filing : 02.07.1999

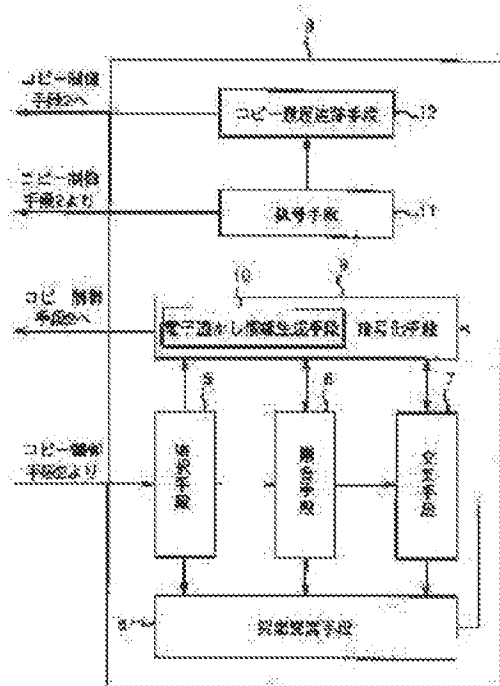
(72)Inventor : KUGA SHIGEKI

(54) CONTENTS DISTRIBUTION CONTROL DEVICE AND PROGRAM RECORDING MEDIUM

(57) Abstract:

**PROBLEM TO BE SOLVED:** To make it possible to inhibit illegal copy, and to ascertain the source of the illegal copy.

**SOLUTION:** When the ID of a copy requesting device is not registered in copy limitation information, a copy control means rejects the request for copy judging it as illegal. A copy history tracing means 12 of the contents distribution control information recording means 3, while comparing the history of contents DNA accumulated in the contents with the original contents DNA of the copying device, performs inverse procedures of harmonization by a harmonization means 6 and crossing by a crossing means 7 until it finally arrives at the original contents DNA of said contents. Thus, the source of the illegal copy is ascertained by extracting the original contents DNA of the copy device which has copied said contents.



\* NOTICES \*

JPO and INPIT are not responsible for any damages caused by the use of this translation.

1. This document has been translated by computer. So the translation may not reflect the original precisely.

2. \*\*\*\* shows the word which can not be translated.

3. In the drawings, any words are not translated.

## DETAILED DESCRIPTION

---

[Detailed Description of the Invention]

[0001]

[Field of the Invention] This invention is accumulated into contents by setting contents distribution management information as the subject of the copy of digital contents (only henceforth contents), or the target of a contents copy. It is related with the contents distribution management device which pursues a copy subject from prevention of the illegal copy of contents, or the copied history of contents.

[0002]

[Description of the Prior Art] These days, contents are in the tendency which is unjustly copied via a network or a recording medium, and spreads with the spread of digital contents. Then, an economic organization, a working group, etc. are established for every peculiar recording medium or contents, and the preventive measure of the illegal copy is devised.

[0003] By history \*\* of 'Takahashi, the anti-copying art of "IEEE1394 written by Naoki Asami, and a public key / common key concomitant use, for example, unification" Nikkei BP, Nikkei electronics In 1998.3.23(No.712)pp.47-pp.53." The prevention art of the 1st illegal copy as shown in the following proposed by CPTWG (Copy Protection Technical Working Group) as the anti-copying method of IEEE1394 is indicated.

[0004] That is, the information called CCI (copy control information) to contents is embedded first. Next, it is investigated whether if there is a demand of the copy from a user, the apparatus of the transmitting side which transmits contents can be copied with reference to the above CCI. Here, CCI comprises 2-bit information and the significance [CCI] is given with the value of 2 bits by 'a copy is impossible', 'only once being copied', 'the copy beyond this not being accepted', and four kinds of the ability 'for any number of times to be copied (copy permission)'.

[0005] Next, the apparatus of the above-mentioned transmitting side performs attestation which checks whether the apparatus of the receiver is provided with anti-copying art. Full attestation and the attestation with restriction are one of the above-mentioned attestation. And when the both sides of the transmitting side and a receiver have a public key, it is considered as full attestation formation. In the above-mentioned full attestation, it controls to transmit the data of the contents which the copy accepted and do not shine. On the other hand, in the attestation with the above-mentioned restriction, when a copy is accepted, the contents of the above CCI control so that only 'only once being copied' and the case of 'any number of times can be copied' transmit contents.

[0006] Here, although the contents to which the copy was accepted may send out data, without enciphering, when transmitting and receiving the data in which the copy is not accepted, encryption is always needed. And the enciphered contents will decrypt by a public key.

[0007] By the above-mentioned CPTWG, CSS (content scrambling system) is determined about DVD (digital video disc) as prevention art of the 2nd illegal copy. In this CSS, four kinds of anti-copying policies are given. A one-eyed preventive measure is called contents encryption, and enciphers contents combining the three enciphering keys a 'master key', a 'disk key', and a 'title key'. In that case, the above 'disk key' and a 'title key' are embedded to the field of DVD which cannot be read via logic file systems, such as a personal computer (it is hereafter called a personal computer for short), with contents.

[0008] The second preventive measure is the reproduction restrictions by a regional code. This is realized by embedding the regional code of the area which sold the DVD device at the circuit and firmware of a DVD device.

[0009] The third preventive measure is APSs (analog protection system). This APS is for performing the copy restrictions to analog VTR (video tape recorder) etc.

It is incorporated and used for the output circuit of the television video signal by hardware.



[0010]The fourth preventive measure is anti-copying policies by bus attestation.

It is treatment technique peculiar to the DVD device carried in the personal computer etc.

In this bus attestation, it checks whether the partner has received the CSS license with the DVD device and the CSS module (or DVD decryption board), and it is made not to perform data transfer until it turns out that the partner has received the CSS license. In that case, the DVD device and the CSS module are sharing the enciphered key data which changes each time "bus key (Bus Key)". And in transmitting the above "disk key" and a "title key" to a CSS module from the above-mentioned DVD device, tapping of a "disk key" and a "title key" is prevented by transmitting, after enciphering by a "bus key" ("it is a prospect to the illegal-copy-prevention art which grasps the key to software decoding.") Nikkei BP, the Nikkei electronics, 1997.8.18(No.696)pp.110-pp.120.

[0011]There is art which inserts digital watermarking in the audio, the picture, the image, or multimedia data indicated by JP,9-191394.A as prevention art of the 3rd illegal copy. According to the gazette, the sequence of the picture, the audio signal, or the image was preferably decomposed by spectrum frequency resolution, and digital watermarking is realized by embedding an identifier peculiar in an important ingredient perceptually [ a decomposition portion ].

[0012]In one side, the art of specifying the root of animals and plants from DNA (deoxyribonucleic acid: one of the genetic materials) of animals and plants is known. For example, following parents to "the Kodansha blue back [ Takao Kuriyama work / "or / what is known by DNA /" ], and 1995" one after another from DNA, and specifying the eve which is human beings' root as them is indicated. The artificial generation method of the decussation and mutation about heredity is indicated to "the Melanie Mitchell work "method of genetic algorithm" TOKYO ELECTRIC university, 1997", etc.

[0013]

[Problem(s) to be Solved by the Invention]However, there are the following problems in the prevention art of the above-mentioned conventional illegal copy. That is, in the prevention art of the above 1st and the 2nd illegal copy, there is a problem of the thing aiming at prevention of an illegal copy that an illegal copy may be indefinitely performed once an illegal-copy-prevention measure is broken, first. A chief aim is placed by preventing an illegal copy, and when an illegal copy is performed, there is also a problem that it cannot be traced where the source of release of an illegal copy is. Although embedded to the field which cannot read the information concerning anti-copying via logic file systems, such as a personal computer, For example, there is a problem that it is also possible to read if ICE (in-circuit emulator), a logic analyzer, etc. of a microprocessor are used, and prevention of the illegal copy to those who have a know how is not thoroughgoing.

[0014]in the prevention art of the illegal copy of the above 1st, since one CCI is assigned to one contents and is in them, there is a problem that tolerance is completely low, to the partial illegal copy in one contents. In the prevention art of the illegal copy of the above 1st, the method of mounting the algorithm of an illegal copy as hardware is going to be taken. However, a logic analyzer can be applied to the parallel interface which connects between LSI for code release (large scale integration circuit), and LSI for decryption, such as an image, also in this case, for example, and the data stream after code release can be taken. Or if an image capture board is connected to the dedicated bus for image transmission which connects decryption LSI and graphics accelerator LSI, there is a problem that it can copy illegally easily.

[0015]On the other hand, in the prevention art of the illegal copy of the above 3rd, there is a problem that the illegal copy of what can lower the quality of the contents copied illegally extremely itself cannot be forbidden. As well as the case of the prevention art of the above 1st and the 2nd illegal copy when an illegal copy is performed, there is a problem that the information concerning the source of release cannot be acquired.

[0016]By the way, the above-mentioned DNA is one of the information effective in specifying parents and the root of animals and plants. However, about the art of using information like DNA as circulation of contents, or information on copy management, it is not yet opened to the public.

[0017]Then, the purpose of this invention forbids an illegal copy, and when an illegal copy is performed, there is in providing the contents distribution management device which can trace that source of release, and the program recording medium with which the contents distribution management program was recorded.

[0018]

[Means for Solving the Problem]In order to attain the above-mentioned purpose, a contents distribution management device of the 1st invention, A memory measure which memorizes information in connection with distribution management of contents or contents, Are the information showing the history of information and a copy subject who express the history of the above-mentioned contents as a copy control means to control copy execution of the above-mentioned contents, and contents distribution management information which can function as copied history information is generated, It is characterized by having a contents distribution management information recording device recorded on a copy object field of both contents of a copied material and a copy destination.

[0019]According to the above-mentioned composition, if a copy of contents is permitted by a copy control means, contents distribution management information will be generated by contents distribution management information recording device, and it will be recorded on a copy object field of the above-mentioned contents. Therefore, it becomes possible to pursue a history of a copy and to specify a copy subject based on contents distribution management information currently recorded on contents copied unjustly or its copy object field. In this way, a source of release of an illegal copy can be traced.

[0020]As for the above-mentioned contents distribution management information recording device in the 1st above-mentioned invention, it is desirable to multiplex and record the above-mentioned contents distribution management information.

[0021]According to the above-mentioned composition, it becomes possible to multiplex information showing the history of the above-mentioned contents, and information showing the above-mentioned copy subject's history, and to consider it as one contents distribution management information. Therefore, relation between the above-mentioned contents and a copy subject is solved by analyzing the above-mentioned contents distribution management information.

[0022]The 1st above-mentioned invention to the above-mentioned contents distribution management information recording device. A selecting means which chooses and reads single information from contents distribution management information currently multiplexed and recorded on a copy object field of the above-mentioned contents in the case of copy execution. It is desirable to have a merging means which generates the multiplexed new contents distribution management information based on information on one layer chosen [ above-mentioned ] and information showing the history of a copy subject who performs a copy.

[0023]According to the above-mentioned composition, information showing the history of the above-mentioned contents and information showing the above-mentioned copy subject's history multiplex, and one contents distribution management information is generated. Therefore, it is easily solved by analyzing the above-mentioned contents distribution management information whether which contents were copied by which copy subject.

[0024]that time -- the above -- newly generated contents distribution management information has the same amount of information as contents distribution management information of origin currently recorded on a copy object field of the above-mentioned contents. Therefore, even if copy operation is repeated, the above-mentioned amount of information is kept constant, and hysteresis information of a copy does not

increase.

[0025]The 1st above-mentioned invention is provided with a decussation means to perform decussation which exchanges a part of information between information which accomplishes a pair which constitutes contents distribution management information generated by the above-mentioned merging means. As for the above-mentioned contents distribution management information recording device, it is desirable to record contents managing distribution information which it crossed [ above-mentioned ].

[0026]It is exchanged in a part of information between information which accomplishes a pair whenever according to the above-mentioned composition the above-mentioned contents are copied and contents distribution management information is generated. As a result, information which expresses the history of a copy subject concerning a copy till the present is inserted in either of the information which accomplishes a pair which constitutes the above-mentioned contents distribution management information.

[0027]As for the above-mentioned decussation means in the 1st above-mentioned invention, it is desirable to control a position of decussation between information which accomplishes the above-mentioned pair, width of decussation, and occurrence frequency of decussation based on a decussation function set up beforehand.

[0028]According to the above-mentioned composition, a position of the above-mentioned decussation, width of decussation, and occurrence frequency of decussation are controlled so that it is inserted in the above-mentioned contents distribution management information, without losing information which expresses the history of all the copy subjects concerning a copy till the present and the contents become ambiguous.

[0029]The 1st above-mentioned invention is provided with a mutation means to which a part of contents distribution management information generated [ above-mentioned ] is mutated, and, as for the above-mentioned contents distribution management information recording device, it is desirable to record contents managing distribution information which it varied [ above-mentioned ].

[0030]According to the above-mentioned composition, the contents of the above-mentioned contents distribution management information are prevented from the disturbance of the contents of the above-mentioned contents distribution management information being carried out, and leaking outside.

[0031]As for the above-mentioned mutation means in the 1st above-mentioned invention, it is desirable to control a position of the above-mentioned variation, the range of variation, and occurrence frequency of variation based on a mutation function set up beforehand.

[0032]According to the above-mentioned composition, a position of the above-mentioned variation, the range of variation, and occurrence frequency of variation are controlled so that the disturbance of the contents of the above-mentioned contents distribution management information is carried out more effectively.

[0033]As for a copy object field of the above-mentioned contents in the 1st above-mentioned invention, it is desirable that it is a unit relevant to structure of the contents concerned.

[0034]According to the above-mentioned composition, the above-mentioned contents distribution management information is recorded in a unit relevant to structure of contents. Therefore, an effect is demonstrated also to a partial illegal copy of contents.

[0035]The 1st above-mentioned invention is provided with an encoding means which enciphers contents distribution management information generated [ above-mentioned ], and, as for the above-mentioned contents distribution management information recording device, it is desirable to record contents managing distribution information enciphered [ above-mentioned ].

[0036]According to the above-mentioned composition, the contents of the above-mentioned contents distribution management information are effectively prevented from disturbance and being concealed and

leaking outside for the contents of the above-mentioned contents distribution management information.  
[0037]The 1st above-mentioned invention is provided with an electronic-watermark-information creating means which generates electronic watermark information based on contents distribution management information enciphered [ above-mentioned ], and, as for the above-mentioned contents distribution management information recording device, it is desirable to record the above-mentioned electronic watermark information.

[0038]According to the above-mentioned composition, the contents of the above-mentioned contents distribution management information are prevented still more effectively [ disturbance and that it is concealed and the contents of the above-mentioned contents distribution management information leak outside ] completely.

[0039]As for the 1st above-mentioned invention, it is desirable to have a copied history tracking means which pursues a history of a copy and specifies a copy subject based on contents distribution management information currently recorded on a copy object field of the above-mentioned contents.

[0040]According to the above-mentioned composition, based on contents distribution management information currently recorded on contents copied unjustly or its copy object field, a history of a copy is pursued by copied history tracking means, and a copy subject is specified by it. In this way, a source of release of an illegal copy is traced easily.

[0041]A decoding means which decrypts contents distribution management information by which the 1st above-mentioned invention is recorded on a copy object field of the above-mentioned contents. It is desirable to have a copied history tracking means which pursues a history of a copy and specifies a copy subject based on contents distribution management information decrypted [ above-mentioned ].

[0042]According to the above-mentioned composition, even if contents distribution management information currently recorded on contents copied unjustly or its copy object field is enciphered, a history of a copy is pursued by copied history tracking means, and a copy subject is specified by it.

[0043]In a specific region which cannot be read in a logic instruction in the above-mentioned memory measure, the 1st above-mentioned invention. Memorize copy limit information including a copy subject's information that a copy was permitted for every contents, and the above-mentioned copy control means. Only when it is the copy subject by whom a demand copy subject is registered into the above-mentioned copy limit information with reference to the above-mentioned copy limit information before performing a copy, the above-mentioned contents distribution management information recording device is ordered generation of the above-mentioned contents distribution management information. As for the above-mentioned contents distribution management information recording device, it is desirable to generate the above-mentioned contents distribution management information based on the above-mentioned instructions.

[0044]According to the above-mentioned composition, by the above-mentioned copy control means, when a copy subject who has advanced a copy demand is a copy subject for copy permission, a copy is permitted. In this way, an illegal copy from a copy subject who is not a candidate for copy permission is prevented. Since the above-mentioned copy limit information is memorized in a specific region which cannot be read in a logic instruction, it cannot be read and altered with the usual copy command.

[0045]As for the above-mentioned copy control means in the 1st above-mentioned invention, when the above-mentioned demand copy subject is a copy subject who is not registered into the above-mentioned copy limit information, it is desirable to forbid execution of a copy or to display a copy prohibition message.

[0046]According to the above-mentioned composition, by the above-mentioned copy control means, when a copy subject who has advanced a copy demand is a copy subject who is not a candidate for copy permission, execution of a copy is forbidden. In this way, an illegal copy from a copy subject to whom a

copy is not permitted is prevented.

[0047]An information storing means which stores copy limit information which includes a copy subject's information that a copy was permitted, for every contents in a specific region where the program recording medium of the 2nd invention cannot read a computer by a logic instruction in a memory measure, A contents distribution management information creating means which generates contents distribution management information which is information showing the history of information and a copy subject showing the history of contents, and can function as copied history information, A decussation means to perform decussation which exchanges a part of information between information which accomplishes a pair which constitutes contents distribution management information generated [ above-mentioned ], A mutation means to which a part of contents distribution management information generated [ above-mentioned ] is mutated, An encoding means which enciphers contents distribution management information generated [ above-mentioned ], An electronic-watermark-information creating means which carries out electronic-watermark-information generation based on contents distribution management information enciphered [ above-mentioned ], and is recorded on a copy object field of both contents of a copied material and a copy destination, A decoding means which decrypts contents distribution management information currently recorded on the above-mentioned contents, and a copied history tracking means which pursues a history of a copy and specifies a copy subject based on contents distribution management information decrypted [ above-mentioned ]. Only when a demand copy subject is a copy subject registered into the above-mentioned copy limit information, it is characterized by recording a contents distribution management processing program and a copied history tracking processing program which perform a copy of the above-mentioned contents and which are operated as a copy control means.

[0048]Information showing the history of a copy subject concerning [ whenever according to the above-mentioned composition the above-mentioned contents were copied and contents distribution management information was generated / till the present ] a copy is inserted in the above-mentioned contents distribution management information. Therefore, based on contents distribution management information currently recorded on contents copied unjustly or its copy object field, a history of a copy is pursued and a copy subject is specified. In this way, a source of release of an illegal copy is traced easily. The contents of the above-mentioned contents distribution management information are effectively prevented from disturbance and being concealed and leaking outside for the contents of the above-mentioned contents distribution management information. An illegal copy in case a copy subject who has advanced a copy demand is a copy subject who is not a candidate for copy permission is prevented.

[0049]

[Embodiment of the Invention]Hereafter, the embodiment of a graphic display of this invention explains in detail. Drawing 1 is a block diagram in the contents distribution management device of this embodiment. Contents, contents distribution management information, and copy limit information are accumulated in the memory measure 1. This memory measure 1 Magnetic memories, such as FD (floppy disk), CD-R (recordable compact disk), MOD (magneto-optics disk), DVD, and a hard disk, Or it realizes by semiconductor memory, such as RAM (random access memory), a smart card, and a flash memory, etc.

[0050]The copy control means 2 controls judgment of copy propriety and copy execution of the above-mentioned contents. The contents distribution management information recording device 3 reads the contents distribution management information of the copy device 4 which is a subject who copies contents or contents, New contents distribution management information is generated using the selecting means, the merging means, the decussation means, mutation means, and encoding means which are explained in full detail behind. And it writes in both the contents of a copied material and a copy destination via the copy control means 2, and the contents of a copy destination are sent out to the copy device 4. The contents distribution management information itself and the contents distribution management information

of the copy device 4 which were generated are recorded and accumulated at the memory measure 1. A copied history is pursued based on the contents distribution management information written in the copied contents. The copy device 4 gives the copy demand of some contents or contents to the copy control means 2, and copies the contents demanded based on control of the copy control means 2.

[0051] The above-mentioned copy control means 2 and the contents distribution management information recording device 3 can be realized by LSI for exclusive use or CPU (central processing unit). The copy device 4 is realized by LSI in which copy execution is possible, CPU, a personal computer, the terminal unit, etc. The copy device 4 may be contained in the inside of this contents distribution management device, and even if constituted from a device other than this contents distribution management device, it does not interfere. Or the memory measure 1 except the copy device 4, the copy control means 2, and the contents distribution management information recording device 3 can also use CPU of other devices, etc.

[0052] Drawing 2 shows the internal structure of the contents distribution management information recording device 3 which is the feature of this invention. The contents distribution management information recording device 3 comprises the selecting means 5, the merging means 6, the decussation means 7, the mutation means 8, the encoding means 9, the decoding means 11, and the copied history tracking means 12.

[0053] The above-mentioned selecting means 5 is changed into single information by choosing one side of the contents distribution management information doubled with this contents distribution management device or the copy device 4. In this embodiment, although it is explained that the above-mentioned contents distribution management information is doubled information, even if it is a case where it multiplexes more than a duplex, it is applicable.

[0054] The above-mentioned merging means 6 unites the contents distribution management information of the copy device 4 selected by the above-mentioned selecting means 5, and the contents distribution management information of the contents used as a copy object. And the doubled new contents distribution management information is generated. Between the contents distribution management information doubled by the merging means 6, the decussation means 7 exchanges a part of mutual information. The mutation means 8 reverses some of values or all values of the above-mentioned contents distribution management information. In this embodiment, since it is inherited leaving the history of the copy into the memory measure 1 contents distribution management information remembered contents or contents to be, there is contents DNA or a case where it is only called DNA for short, about the thing of contents distribution management information henceforth.

[0055] The above-mentioned encoding means 9 is a stage of the input of contents distribution management information, or an output over the above-mentioned selecting means 5, the merging means 6, the decussation means 7, or the mutation means 8, and enciphers to contents distribution management information (contents DNA). The above-mentioned encryption is good in a multiple-times line about each above-mentioned means 5-8. The kind of the above-mentioned encryption is not an object of this invention. It has the electronic-watermark-information creating means 10, and electronic watermark information is generated based on enciphered contents DNA.

[0056] The above-mentioned decoding means 11 decrypts contents DNA which was enciphered by the above-mentioned encoding means 9, and was electronic-watermark-information-ized by the electronic-watermark-information creating means 10. Based on decrypted contents DNA, contents have been copied in what kind of order, or the subject of a copy is whom or the copied history tracking means 12 pursues the copied history of \*\*. This processing is explained in full detail behind.

[0057] Drawing 3 shows the above-mentioned contents DNA and an example of the encryption. Drawing 3 (a) is an example of contents DNA, and is a symbol string showing the history or ID (identifier) of contents or the copy device 4. Although drawing 3 (a) shows the example at the time of using the ID



number of contents or the copy device 4 as the above-mentioned symbol string, even if it is a specific sign, a specific keyword, etc., without being caught by a number, it does not interfere at all.

[0058]Drawing 3 (b) shows the result of having enciphered contents DNA shown in drawing 3 (a) by the above-mentioned encoding means 9. This encryption is performed using the key generated based on the specific function which the encoding means 9 holds. However, in drawing 3 (b), it is changing and displaying on the character string by 8 bitwises so that the obtained code can be viewed. Drawing 3 (c) starts the portion of the beginning of the character string shown in drawing 3 (b), in order to simplify future explanation. Henceforth, it explains as a thing representing the whole information showing contents DNA enciphered in the character string of drawing 3 (c). The character string of explanation which changed the above-mentioned code by 8 bitwises for convenience is treated as a contents DNA. Drawing 3 (d) shows that contents DNA of drawing 3 (c) doubles and is saved.

[0059]Drawing 4 shows changes of contents DNA in fusion by the above-mentioned merging means 6, the decussation by the decussation means 7, and the mutation by the mutation means 8. Drawing 4 (a) shows doubled contents DNA. Here, 21 is contents DNA by the side of contents. 22 is contents DNA by the side of the copy device 4 generated like contents DNA21. the case of drawing 4 (a) — the contents side and a copy device — each contents DNA expresses the state where the only same information is accumulated doubly, 4 side.

[0060]Drawing 4 (b) is chosen by the above-mentioned selecting means 5, and either of contents DNA21 by the side of the doubled contents and either of contents DNA22 by the side of the doubled copy device 4 by the merging means 6. The state where new contents DNA doubled by contents DNA23 by the side of the contents chosen [ above-mentioned ] and contents DNA24 by the side of the copy device 4 was generated is shown.

[0061]Drawing 4 (c) shows the state where decussation was performed by the decussation means 7, to between new contents DNAs generated by the above-mentioned merging means 6. Decussation in this case is performed by replacing five characters from the mutual left end in contents DNA23 by the side of the contents shown in drawing 4 (b), and contents DNA24 by the side of the copy device 4. Henceforth, it is referred to as 'Crossing' to replace partial character strings in this way. That is, that to which five characters intersected five characters from the left end of contents DNA24 from the left end of contents DNA23 is contents DNA25, and that to which five characters intersected five characters from the left end of contents DNA23 from the left end of contents DNA24 conversely is contents DNA26.

[0062]Drawing 4 (d) shows the state where mutation was performed by the above-mentioned mutation means 8. The mutation in this case is a case where a part of information on contents DNA25 shown in drawing 4 (c) changed suddenly, and is set to contents DNA27. In this case, the partial information 'character string ZZ' Becoming is changing to the information 'character string ZY' Becoming.

[0063]Drawing 5 is a key map showing the state where the above-mentioned decussation was performed to the above-mentioned contents DNA. Although the kinds of the above-mentioned decussation include one-point decussation, two-point decussation, uniform decussation, etc., the kind in particular of decussation is not asked in this embodiment. In the case of two-point decussation, in this embodiment, it explains as an example. 'Decussation' is performed when the information on some fields of a certain contents DNA replaces the information on a field that contents DNA which is a pair corresponds.

[0064]In drawing 5, 31 shows contents DNA after decussation was performed. And the information 32 and the information 34 in contents DNA31 are information on the original contents DNA. The information 33 which gave the slash is information replaced from contents DNA which is a pair by decussation.

[0065]The above-mentioned information 33 here probability  $p_c$ , which has the width of  $l_1$  in the position of  $l_0$  and intersects it from the left end of contents DNA31. Probability that the decussation itself will occur is made into  $p_o$ , and probability that decussation information has width  $l_1$  is made into  $p_w$ , and if decussation

makes  $p_i$  probability generated in the position of  $l_j$  from a left end, it can express with  $p_c = p_o * p_w * p_i$ . Similarly, the above-mentioned mutation is also generated in probability  $p_m$ . Probability  $p_o$  and  $p_m$  which decussation and mutation generate are set up by the probability generator in the decussation means 7 and the mutation means 8, respectively.

[0066] Drawing 6 is a flow chart of the contents distribution management information recording processing operation performed by the above-mentioned contents distribution management information recording device 3 under control of the above-mentioned copy control means 2. Hereafter, according to drawing 6, contents distribution management information recording processing is explained.

[0067] At Step S1, it is distinguished by the above-mentioned copy control means 2 whether there is any copy demand from the copy device 4. And if there is a copy demand, it will progress to Step S2. Here, although it may be carried out to some of cases where the above-mentioned copy demand is given to the whole contents, and contents, in order to explain simply, explain the case where it carries out to the whole contents to an example. About the case where a copy demand is performed to some contents, it explains supplementarily behind.

[0068] Collation of contents DNA is performed by the above-mentioned copy control means 2 at Step S2. Contents DNA compared is contents DNA of the both sides from the copy device 4 side which sent out the copy demand the contents side. Contents DNA by the side of contents is written in contents in form as shown in drawing 3 (d), and is memorized by the memory measure 1. [ at least ] On the other hand, contents DNA by the side of the copy device 4 does not necessarily interfere, even if information is information on form as not multiplexed, for example, shown in drawing 3 (a) or drawing 3 (b).

[0069] The propriety of a copy is distinguished based on the copy condition of compatibility read from contents or the memory measure 1 to contents DNA written in and accumulated in the contents side by the above-mentioned copy control means 2 at Step S3, and contents DNA by the side of the copy device 4. And when a copy is good, it progresses to step S4, and in being copy no, it progresses to Step S13. Distinction of this copy propriety is described separately.

[0070] By step S4, according to the copy permission command from the above-mentioned copy control means 2, one is chosen by the selecting means 5 of the contents distribution management information recording device 3 from contents DNAs by the side of the multiplexed contents, and contents DNA is one layer-ized. Each multiplexed contents DNAs are not necessarily the same information, and inside information differs as it goes the generation of a copy in piles.

[0071] Fusion processing which generates contents DNA which multiplexed contents DNA by the side of the contents one layer-ized in step S4 by the above-mentioned merging means 6 at Step S5 combining contents DNA by the side of the copy device 4 is performed.

[0072] The decussation probability parameter of contents DNA is generated by the above-mentioned decussation means 7 at Step S6. Here, as the above-mentioned decussation probability parameter, decussation probability-of-occurrence  $p_o$  mentioned above, probability  $p_i$  of a position, and width probability  $p_w$  are used. Decussation processing is performed by the decussation means 7 at Step S7. That is, the position and width of decussation are determined based on the probability parameter generated in Step S6, and decussation is performed between contents DNA by the side of the contents doubled according to probability-of-occurrence  $p_o$  (multiplexing), and contents DNA by the side of the copy device 4.

[0073] The mutation parameter of contents DNA is generated by the above-mentioned mutation means 8 at Step S8. Here, as the above-mentioned mutation parameter, probability  $q_n$  of a number besides probability-of-occurrence  $q_o$  of mutation, probability  $q_i$  of a position, and width probability  $q_w$ , etc. exist. By step S9, mutation processing is performed by the mutation means 8 based on the above-mentioned mutation parameter. It is determined as which contents DNA of contents DNA by the side of the contents



doubled on that occasion (multiplexing), and contents DNA by the side of the copy device 4 whether mutation is generated.

[0074]Contents DNA is enciphered by the above-mentioned encoding means 9 at Step S10. Here, in this embodiment, a problem is not used in particular about a cipher system. In the flow chart shown in drawing 6, encryption processing is performed only once after mutation. However, contents referred to in this invention or ID of the subject of a copy (drawing 3, (b)), It is possible to contents DNA before performing decussation processing, contents DNA after performing decussation processing, contents DNA after performing mutation processing, etc. 1 time or to carry out multiple-times execution.

[0075]Electronic watermark information is generated from contents DNA enciphered by the above-mentioned electronic-watermark-information creating means 10 in the above-mentioned step S10 at Step S11. In this case, it is also possible to constitute the method of spacing which is different according to the kind of contents so that the electronic-watermark-information creating means 10 may be expressed later selectable. Recording processing which records the electronic watermark information (contents DNA) which serves as the copied history information from the contents distribution management information recording device 3 by the copy control means 2 at Step S12 is performed. 'Records of contents DNA' said here is the processing which is written in the contents of a copy destination and returned to the copy device 4, the processing added and written in the contents of the copy origin memorized by the memory measure 1, and processing saved directly at the memory measure 1.

[0076]Copy execution is prevented when it is distinguished from copy no in the above-mentioned step S3 at Step S13.

[0077]In the flow chart of the above-mentioned contents distribution management information recording processing operation, When a copy is good, encryption is performed by the encoding means 9 after one layer-izing of the information by the selecting means 5, fusion processings by the merging means 6, decussation processings by the decussation means 7, and all the mutation processings by the mutation means 8 are performed. However, the contents distribution management information recording processing operation in this embodiment is not what is limited to this. One layer-izing of information -> various contents distribution management information recording processings, such as encryption, one layer-ized -> fusion processing -> encryption of information, one layer-ized -> fusion processing -> decussation processing -> encryption of information, one layer-ized -> mutation processing -> encryption of information, and one layer-ized -> fusion processing -> mutation processing -> encryption of information, are possible.

[0078]Drawing 7 shows an example of the header information added to each contents, in order to manage contents. This header information is accumulated in the memory measure 1 with the contents added.

[0079]In drawing 7, the record which begins from 'the kind m of contents' and finishes at 'the term of protection m' holds the copyright information of works. Among these, the record 59 is the copyright information about original works, and the records 60 and 61 are the copyright information about secondary works. The records 41, 47, and 53 are the information showing 'content ID m'. The ID number for identifying contents is registered into this record. The above-mentioned ID number may be the identifier which combined the serial order of the row of the number of the media concerned, and content ID. In that case, since it can determine in order of a row, content ID may be omitted.

[0080]The records 42, 48, and 54 express 'the kind (contents type) m of contents'. For the contents protected under copyright in this embodiment, in the kind of contents. The works of a novel, a scenario, a paper, a lecture and other linguistic works, and music, There are a dance or the works of a pantomime, pictures, a print, sculpture and the works of other fine arts, the works of construction, a map, the drawing that has scientific character, a chart, a model and works of other figures, works of a movie, works of a photograph, works of a program, etc. Although the kind of these contents may differ in an object for a

while by the country where contents were produced, or the country consumed, there is no change in the essence of an invention.

[0081]The records 43-45, the records 49-51, and the records 55-57 express the "author" corresponding to the kinds 42, 48, and 54 of contents, respectively. For an author, the number is decided by a common author's existence. For example, for p person and the common authors 49-51 of the secondary works 60, the common author of original works of q person and the common authors 55-57 of the secondary works 61 is r person. An author's records 43-45, 49-51 and the information registered into 55-57 can specify an author, and has some (assumed name) which replace with a name, a name (real name) or its pseudonym, a pen name, an abbreviation, and other real names, for example, are used. Or it may be an ID code which can specify the combination of these and other attributes, such as an address and an occupation, or these authors. An author changes also with the kinds of contents. For example, when the kind of contents is a movie, as an author, it takes charge of work, a supervisor, production, photography, fine arts, music, etc., and what contributed to overall formation of the works about the movie creatively corresponds. When the kind of contents is music, an author deserves a composer, a songwriter, an arrangement house, a player, a singer, etc., and in being a novel, an author deserves a writer, a translator, a sentence painter, etc.

[0082]The records 46, 52, and 58 are the information showing the "contents term of protection m" corresponding to the content ID 41, 47, and 53, and the final day of the shelf-life is usually registered.

[0083]Here, the unit and structure of contents change with the above-mentioned content ID and kinds of contents. For example, when the kinds of contents are linguistic works (it may be henceforth called a document or a document), there are structures other than content ID which show the whole document, such as a table of contents, a chapter, a paragraph, a page, an index, a paragraph, a line, and a character. A copy demand at the above-mentioned step S1 in the contents distribution management information recording processing operation shown in drawing 6 is given to one unit or two or more units by making the above-mentioned structure into a unit. Therefore, the demand of a field copy is also attained like [ "from the 5th paragraph to the 8th paragraph of Chapter 1" ] by specifying the above-mentioned unit other than a copy demand to the whole contents as a copy demand from the copy device 4. [ in the contents whose content ID is "n", for example ]

[0084]Next, in the above-mentioned step S11 in the contents distribution management information recording processing operation shown in drawing 6, the electronic-watermark-information generation processing performed by the above-mentioned electronic-watermark-information creating means 10 is explained in detail. Drawing 8 is a flow chart of electronic-watermark-information generation processing operation. In the above-mentioned step S10 in the flow chart of drawing 6, an end of encryption processing will start electronic-watermark-information generation processing operation.

[0085]At Step S21, the copy object of the copy demanded from the above-mentioned copy device 4 is referred to. At Step S22, the range of a copy demanded from the copy device 4 is referred to. At Step S23, the contents type (kind of contents) of the copy object demanded from the copy device 4 is referred to. These references are performed to the header information of each contents stored in the memory measure 1. And concrete information (contents) is acquired as a result of above reference.

[0086]At Step S24, it is distinguished whether the kind of the reference result in the above-mentioned step S21 - Step S23 and contents is an "image." As a result, if it is an image, it will progress to Step S25, otherwise, will progress to Step S28. It is distinguished at Step S25 whether the kind of contents is a "still picture." As a result, if it is a still picture, it will progress to Step S26, otherwise, will progress to Step S27. The still picture watermark method is chosen at Step S26. To such the back, it goes at Step S33. Here, a concentration-patterns method, systematic dithering method, an error diffusion method, etc. exist in the still picture watermark method. And when image data has shade information, how to space various kinds, such as pixel substitution, pixel space use, quantization error use, frequency domain use, and

statistics value use, is known. In this embodiment, specification in particular is not carried out about the still picture watermark method. The animation watermark method is chosen at Step S27. To such the back, it goes at Step S33. Here, the method of spacing according to standards, such as MPEG(moving picture extract part group) 1, MPEG 2, and MPEG4, is known by the animation watermark method. In this embodiment, specification in particular is not carried out about the animation watermark method.

[0087]It is distinguished at Step S28 whether the kind of contents is a "sound." As a result, if it is a sound, it will progress to Step S29, otherwise, will progress to Step S30. The voice watermark method is chosen at Step S29. Such the back progresses to Step S33. Here, the method of analog format, voice quantization, aural masking, a prediction numerals run length, vector quantization, a sound source pulse, etc. spacing through the voice watermark method is known. In this embodiment, specification in particular is not carried out about the voice watermark method.

[0088]It is distinguished at Step S30 whether the kind of contents is a "document." As a result, if it is a document, it will progress to Step S31, otherwise, will progress to Step S32. The document watermark method is chosen at Step S31. To such the back, it goes at Step S33. Here, the method of spacing through the document watermark method in European languages or Japanese, and changing the generation technique is known. At Step S32, the method of spacing according to other "kinds of contents" is chosen. Like \*\*\*\*, in this embodiment, a problem is not used about the digital-watermarking method, but at least one digital-watermarking method should just be chosen according to the kind of contents.

[0089]It is distinguished whether electronic watermark information is generable by the method selected at Step S33 as mentioned above of spacing. As a result, if generation is possible, it will progress to Step S36, and if generation is impossible, it will progress to Step S34. Here, the electronic watermark information written in a copy object in this embodiment is contents DNA which has specified length. Therefore, since a copy unit (getting it blocked the range of a copy object) cannot write in the electronic watermark information acquired when small enough compared with contents DNA, it judges with generation of electronic watermark information being impossible. In a watermark information writing area, it is distinguished at Step S34 whether it is the maximum. As a result, if it is the maximum, a return will be carried out to the above-mentioned step S13 in the above-mentioned contents distribution management information recording processing operation, and the copy concerned will be refused. On the other hand, if it is not the maximum, it will progress to Step S35. Here, the maximum of the above-mentioned watermark information writing area is the whole contents of the content ID which is a copy object.

[0090]At Step S35, the above-mentioned electronic-watermark-information writing area is expanded to the field (large one unit) on one rank rather than the present field. Here, the initial value of an electronic-watermark-information writing area is the copy range (unit) obtained as a result of the reference in the above-mentioned step S22. Such the back returns to the above-mentioned step S23, and selection of the digital-watermarking method is performed again. And if it judges that electronic watermark information is [ generation ] possible in the above-mentioned step S33, it will progress to Step S36.

[0091]At Step S36, a digital-watermarking writing area is determined based on the present watermark information writing area. At Step S37, the electronic watermark information of contents DNA is generated by the digital-watermarking method chosen [ above-mentioned ]. In such the back, a return is carried out to the above-mentioned step S12 in the above-mentioned contents distribution management information recording processing operation, and recording processing is performed. As a result, the electronic watermark information of contents DNA generated in the above-mentioned step S37 is written in the digital-watermarking writing area determined in the above-mentioned step S36 in both the contents of a copied material and a copy destination. And the contents of the copy destination where this contents DNA (electronic watermark information) was written in are returned to the copy device 4.

[0092]Next, the processing which pursues a copied history is explained based on contents DNA

(electronic watermark information) written in contents as mentioned above. Drawing 9 shows changes of contents DNA when one contents are copied one by one. 65 in drawing 9 is contents DNA of the original copy (the 1st generation) in contents. Similarly, 66 is original contents DNA in copy device A, 67 is original contents DNA in copy device B, and 68 is original contents DNA in copy device C.

[0093]The merging means's 6 fusion of original content DNA by the side of contents and original content DNA of copy device A will generate contents DNA69 of the second generation. A figure shows that original content DNA of each origin has accomplished the pair. Contents DNA70 will be generated if decussation is performed by the decussation means 7 to this contents DNA pair. Into the information which is the target of the above-mentioned decussation, \*\*\*\*\* also includes and explains to decussation that by which a part of information was changed by the above-mentioned mutation henceforth.

[0094]Next, if fusion is performed between second generation contents DNA70 after the above-mentioned decussation, and original content DNA67 of copy device B, contents DNA71 of the third generation will be generated. And contents DNA72 will be generated if decussation is performed to the contents DNA pair of contents DNA71. Similarly, if fusion is performed between third generation contents DNA72 after decussation, and original content DNA68 of copy device C, contents DNA73 of the fourth generation will be generated. And contents DNA74 will be generated if decussation is performed to the contents DNA pair of contents DNA73.

[0095]Saying "a copied history is pursued" in this embodiment. Contents DNA74 of the fourth generation after decussation being given, and following changes of contents DNA73 of the fourth generation before decussation, contents DNAs 72 and 71 of the third generation decussation back to front, contents DNAs 70 and 69 of the second generation decussation back to front, and contents DNA. It is clarifying the copy devices A-C (original content DNAs 66-68) which participated in the copy.

[0096]Drawing 10 is a flow chart of the copied history tracking processing operation performed by the contents distribution management information recording device 3 under control of the above-mentioned copy control means 2. Hereafter, copied history tracking processing is explained according to drawing 10. Contents DNA which becomes the origin of the pursuit in that case should be generated in order of the copy in drawing 9.

[0097]The contents DNA74 [ newest ] is extracted out of contents DNA written in and accumulated in the contents or the memory measure 1 which is the target of pursuit by the above-mentioned copy control means 2 at Step S41. Here, the selection of the newest contents DNA should just choose contents DNA with the most complicated both sides of contents DNA that accomplish a pair. What is necessary is just to create the index of the order of a copy, and the writing address of contents DNA, when accumulating contents DNA in contents in order to accelerate extraction of the newest contents DNA.

[0098]The contents DNA74 [ newest ] extracted in the above-mentioned step S41 at Step S42 by the decoding means 11 in the above-mentioned contents distribution management information recording device 3 is decrypted. The difference of the contents DNA74 [ newest ] and original content DNAs 66-68 of each copy device A-C which were decrypted by the above-mentioned copied history tracking means 12 in the above-mentioned step S42 at Step S43 is called for. Original content DNAs 66-68 of each copy devices A-C are stored and saved at the memory measure 1, when a copy is performed in the past. Original content DNA which presents the minimum difference at Step S44 is calculated. In this example, when original content DNA68 of copy device C is compared with contents DNA74b [ on the other hand / (in drawing 9, it is the bottom) ] in latest-contents DNA74, it becomes with the minimum difference.

[0099]The preliminary decision of the copy device C of original content DNA68 which presents the minimum above-mentioned difference at Step S45 is carried out as a copy subject. At Step S46, the difference of original content DNA68 of a copy subject by which the preliminary decision was carried out [ above-mentioned ], and above-mentioned one contents DNA74b of latest-contents DNA74 which

presents the above-mentioned minimum difference is taken. As a result, in this example, the lower 1st slash field 75 and the 2nd slash field 76 in contents DNA74b are extracted.

[0100]The compensation process which replaces the information on the fields 75 and 76 extracted in the above-mentioned step S46 at Step S47 with the information on the field 77 in a pair of contents DNA74a (above) that it corresponds is performed. As a result, it is returned to contents DNA73 before contents DNA74 after the decussation which is latest-contents DNA crossing. In that case, bit flipping is carried out so that the degree of match of lower contents DNA73b and original content DNA68 of a copy subject in contents DNA73 before the obtained decussation may become the maximum, and the data modification produced in mutation is also amended. It is distinguished whether contents DNA73b before the decussation obtained at Step S48 as a result of the amendment in the above-mentioned step S47 is in agreement with original content DNA68 of a copy subject. As a result, if, and it progresses to Step S49 and is not in agreement with it, it returns to the above-mentioned step S47, and amendment of the above-mentioned mutation, etc. are continued.

[0101]Contents DNA73 before the decussation obtained as mentioned above at Step S49 as a result of amendment is determined as a contents DNA of present cost. Copy device C which has original content DNA68 of the same contents as contents DNA73b of the bottom in contents DNA73 of the present cost determined [ above-mentioned ] at Step S50 is specified as it is the copy device which participated in generation of contents DNA73 of present cost. At Step S51, contents DNA concerning a previous generation's contents is calculated from contents DNA73a of the upper part in contents DNA73 of present cost.

[0102]It is distinguished whether contents DNA73a concerning a previous generation's contents 73 called for in the above-mentioned step S51 at Step S52 is original content DNA (getting it blocked -- the contents of the 1st generation -- do DNA or not?). As a result, if it is original content DNA, copied history tracking processing operation will be ended. On the other hand, if it is not original content DNA, it will progress to Step S53.

[0103]Previous generation contents DNA72 which has a previous generation's contents DNA73a called for in the above-mentioned step S51 is searched with Step S53 from all the contents DNAs accumulated in the contents concerned, or the above-mentioned index. At Step S54, it is distinguished as a result of the search in the above-mentioned step S53 whether applicable previous generation contents DNA was in the DNA information of the contents concerned. As a result, in being, it returns to the above-mentioned step S43, and shifts to the history tracking processing about a previous generation further. On the other hand, when there is nothing, it progresses to Step S55. In shifting to the history tracking processing about a previous generation further here, it applies 'contents DNA72' to 'the contents DNA74 [ newest ]' in the above-mentioned step S43 and the above-mentioned step S46. And if contents DNA which starts a previous generation's contents in the above-mentioned step S52 is distinguished as it is original content DNA, it will end copied history tracking processing operation. At Step S55, the back copied history tracking processing operation to which the error display was carried out is ended.

[0104]Next, the decision processing of the copy propriety performed in the above-mentioned step S2 and Step S3 in the contents distribution management information recording processing operation shown in above-mentioned drawing 6 is explained in detail. Drawing 11 shows the data structure at the time of recording the limitation information of a copy. This copy limit information is written in the specific region which cannot be read in the usual copy command (getting it blocked logic instruction) in contents or the memory measure 1.

[0105]In drawing 11, the records 81, 88, and 89 are records which record the ID number of copy object contents. The contents of these records 81, 88, and 89 are the same as that of the content ID 41, 47, and 53 in the header information shown in drawing 7. The records 82, 84, 86, 90, and 91 are records which record

ID of the copy device with which the copy of contents was permitted. The records 83, 85, and 87 are records which record the copy restricted frequency by each copy device to the contents concerning the content ID 1. Similarly, the copy restricted frequency according [ copy device ID / as opposed to the contents of 'm' in content ID ] to the copy device of 'x' is recorded on the record 92.

[0106]That is, the copy information 93 is the copy information about the contents whose content ID is '1'. Similarly, the copy information 94 and 95 is the copy information about the contents whose content ID is '2' and 'm'. Each above-mentioned copy information shall be enciphered by the encryption algorithm used when generating contents DNA.

[0107]Drawing 12 is a flow chart of copy propriety decision processing operation. If there is a copy demand in the above-mentioned step S1 in the contents distribution management information recording processing operation shown in above-mentioned drawing 6 and it will be distinguished, the above-mentioned copy propriety decision processing operation will start.

[0108]Specification of a demand copy device which specifies the copy device which performed the copy demand at Step S61 is performed. specification of a demand copy device is written in the above-mentioned specific region in the contents or the memory measure 1 of a copy object -- \*\*\*\* -- it is carried out by referring to copy limit information (drawing 11). This processing is performed before the usual copy command. At Step S62, it is judged whether specification of the demand copy device was successful. As a result, when it succeeds, the copy device which advanced the copy demand is recognized as it being a copy permission object device, and progresses to Step S63. On the other hand, a return is carried out to the above-mentioned step S13 in the above-mentioned contents distribution management information recording processing operation noting that the possibility of an illegal copy is size, when it fails.

[0109]Contents DNA saved in the copy object concerned at Step S63 based on a copy object and ID of the copy device which is the above-mentioned copy permission object device is referred to. Past history decipherment processing in which it is decoded how many times the copy device which has sent out the copy demand at Step S64 this time based on the reference result of the above-mentioned contents DNA copied the copy object concerned in the past is performed. In that case, the method of a decipherment which can be set applies to the copied history tracking processing operation shown in drawing 10.

[0110]At Step S65, the contents of the above-mentioned copy limit information (drawing 11) are referred to. The copy restricted frequency in connection with the copy device and copy object which advanced the demand by Step S66 based on the result of above reference is compared with the copied history of the above-mentioned past, and it is distinguished whether the copy frequency by this demand is below copy restricted frequency. As a result, if it is the following, a return will be carried out to the above-mentioned step S4 in the above-mentioned contents distribution management information recording processing operation, and generation of new contents DNA will be started. On the other hand, if that is not right, a return will be carried out to the above-mentioned step S13 in the above-mentioned contents distribution management information recording processing operation.

[0111]As mentioned above, the memory measure 1 which memorizes and accumulates contents and contents DNA in this embodiment, A copy control means 2 to control judgment of the copy propriety of the above-mentioned contents, pursuit of a copied history, and copy execution, Based on contents and contents DNA of the copy device 4, it has the contents distribution management information recording device 3 which writes in and records new contents DNA on the contents generated and copied.

[0112]And when the above-mentioned contents distribution management information recording device 3 generates contents DNA, One of the contents DNAs by the side of the contents doubled by the selecting means 5 is chosen, it doubles combining contents DNA by the side of the contents chosen [ above-mentioned ] by the merging means 6, and original content DNA by the side of the copy device 4, and new contents DNA is generated. And it crosses to the contents DNA pair in doubled new contents DNA further



by the decussation means 7 of the above-mentioned contents distribution management information recording device 3. It mutates by the mutation means 8 if needed.

[0113]On the other hand, the copy limit information which contains the copy restricted frequency by ID and the copy device of the copy device for copy permission in the specific region which cannot be read in the usual copy command (logic instruction) is written in each contents or the memory measure 1.

[0114]If a copy demand is received from the copy device 4, the above-mentioned copy control means 2 will be made to carry out copy refusal with reference to the above-mentioned copy limit information, when the demand copy device 4 is not a copy permission object device. Therefore, according to this embodiment, the illegal copy can be prevented.

[0115]On the other hand, in being a copy permission object device, it orders it pursuit of a copied history to the contents distribution management information recording device 3. So by then, the copied history tracking means 12 of the contents distribution management information recording device 3. Performing comparison with the history of contents DNA accumulated in the memory measure 1, and original content DNA of the copy device which copied to the past, the above-mentioned fusion, decussation, and the reverse procedure of mutation are followed until it is followed and attached to original content DNA of the contents concerned. As a result, original content DNA by the side of the copy device crossing by the time original content DNA of the contents concerned changed to the newest contents DNA can be extracted.

[0116]Therefore, based on the copy device and copy frequency which copied to the past obtained in this way, the contents of the above-mentioned copy limit information, and ID of the copy device which advances a demand now and is, it can be judged [ which receives the copy demand which acts as Imaide / or or ] whether it refuses. That is, according to this embodiment, even if the metaphor above-mentioned illegal-copy-prevention measure is broken, it can prevent being copied illegally indefinitely.

[0117]When the contents stored in the above-mentioned memory measure 1 are copied unjustly and have appeared on the market in the commercial scene, Based on the history of contents DNA written in and accumulated in inaccurate copy contents, the copy device concerning an illegal copy can be solved by pursuing an above-mentioned copied history. Therefore, the source of release of the illegal copy can be traced.

[0118]In the case of a document or a document, in this embodiment, contents DNA generated at the time of a copy can be written in by contents in the unit relevant to the structure of each contents, such as a table of contents, a chapter, a paragraph, a page, a paragraph, or a line, for example. Therefore, in the unit according to each contents, contents DNA can be embedded and tolerance becomes high also to the partial illegal copy of contents.

[0119]In this embodiment, as mentioned above, when copying contents, decussation processing and mutation processing are performed to required contents DNA. By the encoding means 9 and the electronic-watermark-information creating means 10 of the contents distribution management information recording device 3, contents DNA generated as mentioned above is enciphered and digital-watermarking computerized, and the disturbance and concealment of information are performed. Therefore, even if it reads contents unjustly using apparatus, such as the above-mentioned ICE, it is impossible to decode the contents of the contents DNA or to alter. The above-mentioned copy limit information is written in the specific region which cannot be read in the usual copy command (logic instruction) of contents or the memory measure 1. Therefore, the existence of this copy limit information itself is not clarified.

[0120]In this embodiment, the amount of information of the above-mentioned contents DNA is kept constant by operation of the selecting means 5 and the merging means 6. Therefore, even if it repeats copy operation, the amount of hysteresis information (amount of information of contents DNA) does not increase.

[0121]By the way, the function as the copy control means 2 in the above-mentioned embodiment, the

contents distribution management information recording device 3, the selecting means 5, the merging means 6, the decussation means 7, the mutation means 8, the encoding means 9, the electronic-watermark-information creating means 10, the decoding means 11, and the copied history tracking means 12, The contents distribution management information recording processing program, the electronic-watermark-information generation and the recording processing program and the copied history tracking processing program which were recorded on the program recording medium, and a copy propriety decision processing program realize.

[0122]The above-mentioned program recording media in the above-mentioned embodiment are program media which become by ROM (read only memory; not shown) provided in the different body in the above-mentioned memory measure 1. Or they may be the program media equipped with and read to external auxiliary storage (not shown). The program reading means which reads each above-mentioned processing program from the above-mentioned program media in the case of which, It may have the composition which carries out direct access to the above-mentioned program media, and is read to them, and it may download in the program store area established in RAM (not shown), and may have the composition accessed and read to the above-mentioned program store area. The download program for downloading in the program store area of the above-mentioned RAM from the above-mentioned program media shall be beforehand stored in the main frame.

[0123]With the above-mentioned program media, it is constituted disengageable the main part side here, Magnetic disks, such as a tape system of magnetic tape, a cassette tape, etc., FD, and a hard disk, CD(compact disk)-ROM, MOD, MD (mini disc), It is a medium including semiconductor memory systems, such as card systems, such as a disk system of optical discs, such as DVD, IC (integrated circuit) card, and an optical card, a mask ROM, EPROM (ultraviolet-rays elimination type ROM), EEPROM (electric elimination type ROM), and a flash ROM, which supports a program fixed.

[0124]The contents distribution management device in the above-mentioned embodiment, When it has the composition which is provided with a modem and contains the Internet and in which a communication network and connection are possible, even if the above-mentioned program media are media which support a program fluidly by download from a communication network, etc., they do not interfere. The download program for downloading from the above-mentioned communication network which can be set in that case shall be beforehand stored in the main frame. Or it shall be installed from another recording medium.

[0125]It is not limited only to a program and what is recorded on the above-mentioned recording medium can also record data.

[0126]

[Effect of the Invention]As mentioned above, so that clearly the contents distribution management device of the 1st invention, Contents DNA which is the information showing the history of the information and copy subject showing the history of contents, and can function as copied history information by a contents distribution management information recording device is generated, Since it records on the copy object field of both the contents of a copied material and a copy destination, copied history information will be recorded on the copy object field of the copied contents. Therefore, it becomes possible to pursue the history of a copy and to specify a copy subject based on contents DNA currently recorded on the contents copied unjustly or its copy object field. That is, according to this invention, the source of release of an illegal copy can be traced.

[0127]If the above-mentioned contents DNA is multiplexed and recorded by the above-mentioned contents distribution management information recording device, the 1st above-mentioned invention will multiplex the information showing the history of the above-mentioned contents, and the information showing the above-mentioned copy subject's history, and it will become possible to be referred to as one



contents DNA. Therefore, the relation between the above-mentioned contents and a copy subject can be solved by analyzing the above-mentioned contents DNA.

[0128]The selecting means which chooses single information from contents DNA which multiplexes the 1st above-mentioned invention to the above-mentioned contents to the above-mentioned contents distribution management information recording device in the case of copy execution, and is recorded, If it has a merging means which generates new contents DNA multiplexed based on the information on one layer chosen [ above-mentioned ], and the information showing a copy subject's history, the information showing the history of the above-mentioned contents and the information showing a copy subject's history are multiplexed, and one contents DNA can be generated. Therefore, it can be easily solved by analyzing the above-mentioned contents DNA whether which contents were copied by which copy subject.

[0129]that time -- the above -- newly generated contents DNA has the same amount of information as contents DNA of the origin currently recorded on the copy object field of the above-mentioned contents. Therefore, even if it repeats copy operation, the above-mentioned amount of information can be kept constant, and the hysteresis information of a copy can be prevented from increasing.

[0130]The 1st above-mentioned invention can generate easily contents DNA in which the information which expresses the history of the copy subject concerning a copy till the present was inserted, if a part of information is exchanged between the information which accomplishes the pair which constitutes contents DNA generated by the above-mentioned merging means by a decussation means.

[0131]If the position of decussation between the information which accomplishes the above-mentioned pair, the width of decussation, and the occurrence frequency of decussation are controlled based on the decussation function beforehand set up in the above-mentioned decussation means in the 1st above-mentioned invention, Contents DNA to which it is inserted in, without losing the information which expresses the history of all the copy subjects concerning a copy till the present, and the disturbance of the contents is carried out is generable.

[0132]The 1st above-mentioned invention can prevent the contents of the above-mentioned contents DNA from carrying out the disturbance of the contents of the above-mentioned contents DNA, and leaking outside by a mutation means, if it varies in a part of contents DNA generated [ above-mentioned ].

[0133]If the position of the above-mentioned variation, the range of variation, and the occurrence frequency of variation are controlled based on the mutation function beforehand set up in the above-mentioned mutation means in the 1st above-mentioned invention, the disturbance of the contents of the above-mentioned contents DNA can be carried out more effectively.

[0134]The 1st above-mentioned invention can record the above-mentioned contents DNA in the unit relevant to the structure of contents, if the copy object field of the above-mentioned contents is made into the unit relevant to the structure of the contents concerned. Therefore, tolerance over the partial illegal copy of contents can be made high.

[0135]The 1st above-mentioned invention can do the disturbance and concealment of the contents of the above-mentioned contents DNA, if contents DNA generated [ above-mentioned ] is enciphered by an encoding means. Therefore, the contents of the above-mentioned contents DNA can be effectively prevented from leaking outside.

[0136]In disturbance and concealment, the 1st above-mentioned invention can do the contents of the above-mentioned contents DNA more nearly thoroughly, if an electronic-watermark-information creating means generates electronic watermark information based on contents DNA enciphered [ above-mentioned ]. Therefore, the contents of the above-mentioned contents DNA can be prevented from leaking outside still more effectively.

[0137]If the 1st above-mentioned invention pursues the history of a copy based on the above-mentioned contents DNA currently recorded on the above-mentioned contents and specifies a copy subject by a

copied history tracking means, The history of the copy about the contents copied illegally can be pursued and the source of release of an illegal copy can be traced easily.

[0138]Based on decrypted contents DNA, the 1st above-mentioned invention by a decoding means by a copied history tracking means. If the history of a copy is pursued and a copy subject is specified, even if contents DNA currently recorded on the contents copied unjustly is enciphered, the history of a copy can be pursued and a copy subject can be specified.

[0139]Memorize the 1st above-mentioned invention to the specific region which cannot be read in the logic instruction in the above-mentioned memory measure, and copy limit information including a copy subject's information that the copy was permitted by the above-mentioned copy control means. If the above-mentioned contents distribution management information recording device is ordered generation of the above-mentioned contents DNA only when a demand copy subject is a copy subject registered into the above-mentioned copy limit information, A copy is permitted only to the copy subject for copy permission, and the illegal copy from the copy subject who is not a candidate for copy permission can be prevented. Since the above-mentioned copy limit information is memorized in the specific region which cannot be read in a logic instruction, it can prevent being read and altered with the usual copy command.

[0140]If the 1st above-mentioned invention forbids execution of a copy or it displays a copy prohibition message in being a copy subject by whom the above-mentioned demand copy subject is not registered into the above-mentioned copy limit information in the above-mentioned copy control means, The illegal copy by the copy subject who is not a candidate for copy permission can be forbidden.

[0141]The information storing means which stores the above-mentioned copy limit information in the specific region where the program recording medium of the 2nd invention cannot read a computer by the logic instruction in a memory measure, The contents distribution management information creating means which generates the above-mentioned contents DNA, A decussation means to perform the above-mentioned decussation, a mutation means to perform the above-mentioned mutation, and the encoding means that performs the above-mentioned encryption, The electronic-watermark-information creating means which generates and records the above-mentioned electronic watermark information, The decoding means which decrypts the above-mentioned contents DNA, and the copied history tracking means which pursues the history of a copy and specifies a copy subject, Since the contents distribution management processing program and copied history tracking processing program which perform a copy and which are operated as a copy control means are recorded only when it is the demand from a copy subject registered into the above-mentioned copy limit information, Based on contents DNA currently recorded on the contents copied unjustly, the source of release of an illegal copy can be traced easily.

[0142]The contents of the above-mentioned contents DNA can be effectively prevented from disturbance and concealing and leaking outside for the contents of the above-mentioned contents DNA. The illegal copy by the copy subject who is not a candidate for copy permission can be prevented.

## CLAIMS

---

[Claim(s)]

[Claim 1] A contents distribution management device comprising:

A memory measure which memorizes information in connection with distribution management of contents or contents,

A copy control means to control copy execution of the above-mentioned contents.

A contents distribution management information recording device which is the information showing the history of information and a copy subject showing the history of the above-mentioned contents, generates contents distribution management information which can function as copied history information, and is recorded on a copy object field of both contents of a copied material and a copy destination.

[Claim 2] A contents distribution management device the above-mentioned contents distribution management information recording device's multiplexing the above-mentioned contents distribution management information, and recording it in the contents distribution management device according to claim 1.

[Claim 3] The contents distribution management device comprising according to claim 2:

A selecting means which the above-mentioned contents distribution management information recording device chooses single information from contents distribution management information currently multiplexed and recorded on a copy object field of the above-mentioned contents in the case of copy execution, and is read.

Information on one layer chosen [ above-mentioned ].

A merging means which generates the multiplexed new contents distribution management information based on information showing the history of a copy subject who copies.

[Claim 4] It has a decussation means to perform decussation which exchanges a part of information between information which accomplishes a pair which constitutes contents distribution management information generated by the above-mentioned merging means in the contents distribution management device according to claim 3, A contents distribution management device, wherein the above-mentioned contents distribution management information recording device records contents managing distribution information which it crossed [ above-mentioned ].

[Claim 5] A contents distribution management device, wherein the above-mentioned decussation means controls a position of decussation between information which accomplishes the above-mentioned pair, width of decussation, and occurrence frequency of decussation in the contents distribution management device according to claim 4 based on a decussation function set up beforehand.

[Claim 6] A contents distribution management device, wherein it has a mutation means to which a part of contents distribution management information generated [ above-mentioned ] is mutated in the contents distribution management device according to claim 1 and the above-mentioned contents distribution management information recording device records contents managing distribution information which it varied [ above-mentioned ].

[Claim 7] A contents distribution management device, wherein the above-mentioned mutation means controls a position of the above-mentioned variation, the range of variation, and occurrence frequency of variation in the contents distribution management device according to claim 6 based on a mutation function set up beforehand.

[Claim 8] A contents distribution management device characterized by a copy object field of the above-mentioned contents being a unit relevant to structure of the contents concerned in the contents distribution

management device according to claim 1.

[Claim 9]A contents distribution management device having a copied history tracking means which pursues a history of a copy and specifies a copy subject in the contents distribution management device according to claim 1 based on contents distribution management information currently recorded on a copy object field of the above-mentioned contents.

[Claim 10]In the contents distribution management device according to claim 1, in a specific region which cannot be read in a logic instruction in the above-mentioned memory measure. Copy limit information including a copy subject's information that a copy was permitted is memorized for every contents, and the above-mentioned copy control means, Only when it is the copy subject by whom a demand copy subject is registered into the above-mentioned copy limit information with reference to the above-mentioned copy limit information before performing a copy, the above-mentioned contents distribution management information recording device is ordered generation of the above-mentioned contents distribution management information, A contents distribution management device, wherein the above-mentioned contents distribution management information recording device generates the above-mentioned contents distribution management information based on the above-mentioned instructions.

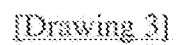
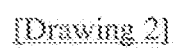
[Claim 11]In the contents distribution management device according to claim 10, the above-mentioned copy control means, A contents distribution management device forbidding execution of a copy or displaying a copy prohibition message when the above-mentioned demand copy subject is a copy subject who is not registered into the above-mentioned copy limit information.

[Claim 12]An information storing means which stores copy limit information which includes a copy subject's information that a copy was permitted, for every contents in a specific region which cannot read a computer by a logic instruction in a memory measure, A contents distribution management information creating means which generates contents distribution management information which is information showing the history of information and a copy subject showing the history of contents, and can function as copied history information, A decussation means to perform decussation which exchanges a part of information between information which accomplishes a pair which constitutes contents distribution management information generated [ above-mentioned ], A mutation means to which a part of contents distribution management information generated [ above-mentioned ] is mutated, An encoding means which enciphers contents distribution management information generated [ above-mentioned ], An electronic-watermark-information creating means which carries out electronic-watermark-information generation based on contents distribution management information enciphered [ above-mentioned ], and is recorded on a copy object field of both contents of a copied material and a copy destination, A decoding means which decrypts contents distribution management information currently recorded on the above-mentioned contents, and a copied history tracking means which pursues a history of a copy and specifies a copy subject based on contents distribution management information decrypted [ above-mentioned ], As a copy control means to perform a copy of the above-mentioned contents only when a demand copy subject is a copy subject registered into the above-mentioned copy limit information. A program recording medium in which computer read-out is possible, wherein a contents distribution management processing program and a copied history tracking processing program to operate are recorded.

---

[Translation done.]

Drawing 11



(a)

50367-851-2655953-04370

(b)

hIwD5PKU2Wx0VCkBA/0ZZtbsz/pDekRErMw0Q4AF1UPdkK  
8DeuhEOXzAq1Ddgj/4  
PLVZEtiAaxarDNjQ8M4Dt7jger4Qat6HUZiRi8C2SjWihvgkahx  
5RPFel+C5aIfz2  
YpRdjZ9LHmNifdCFik+Sow6F3NmAmzXbSEadUmLE8dDwM  
QVwlv7N/UmtT5OS9KYA  
AAA8imhwuvn48Lg6KUqgM6oa5VAu6l4jpcAT14u9OBmqFTb  
2Snf9FDSjydNnx7Ia  
QuH2l4ee6r+qK1HMM/Zr  
=vzhT

(c)

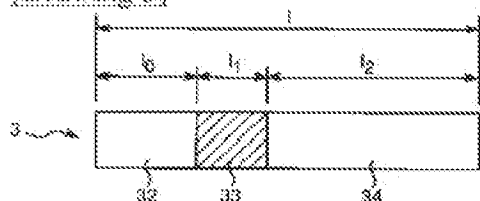
hIwD5PKU2Wx0VCkBA/0ZZtbsz/pDekREr

(d)

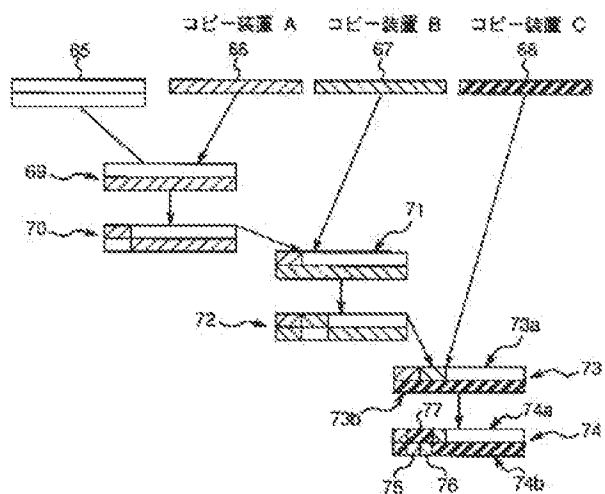
hIwD5PKU2Wx0VCkBA/0ZZtbsz/pDekREr

hIwD5PKU2Wx0VCkBA/0ZZtbsz/pDekREr

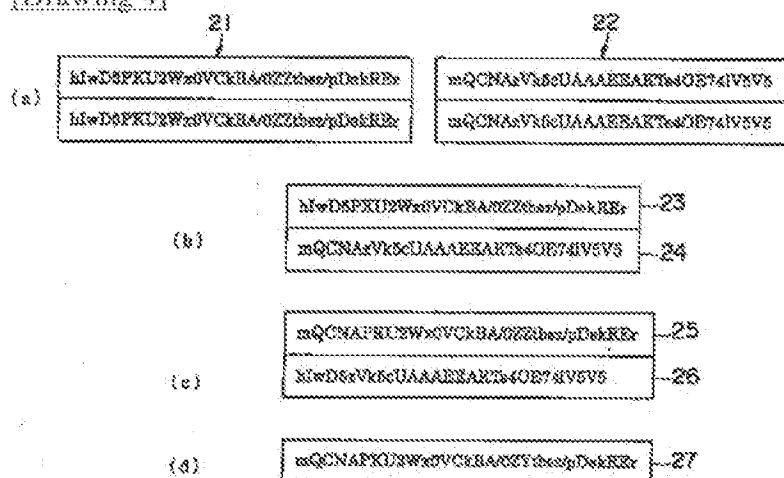
[Drawing 5]



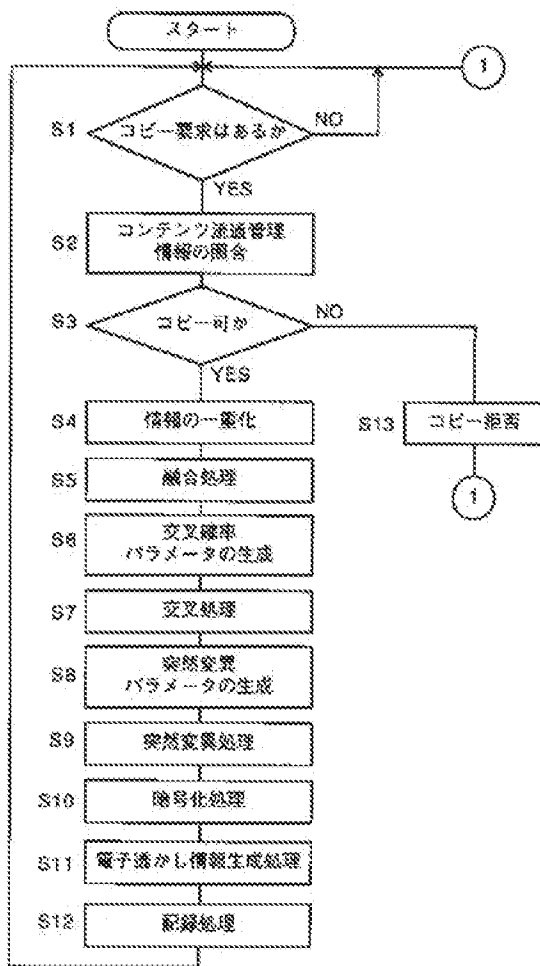
[Drawing 9]



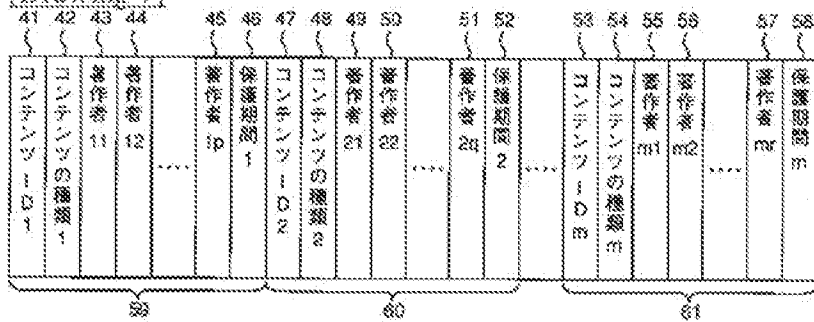
[Drawing 4]



[Drawing 6]



[Drawing 7]

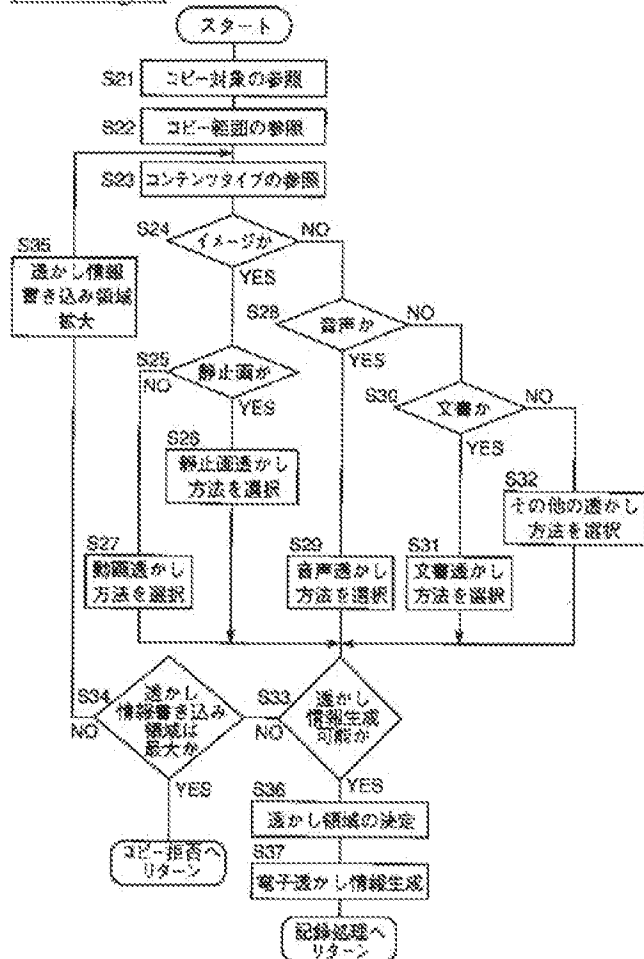


[Drawing 11]

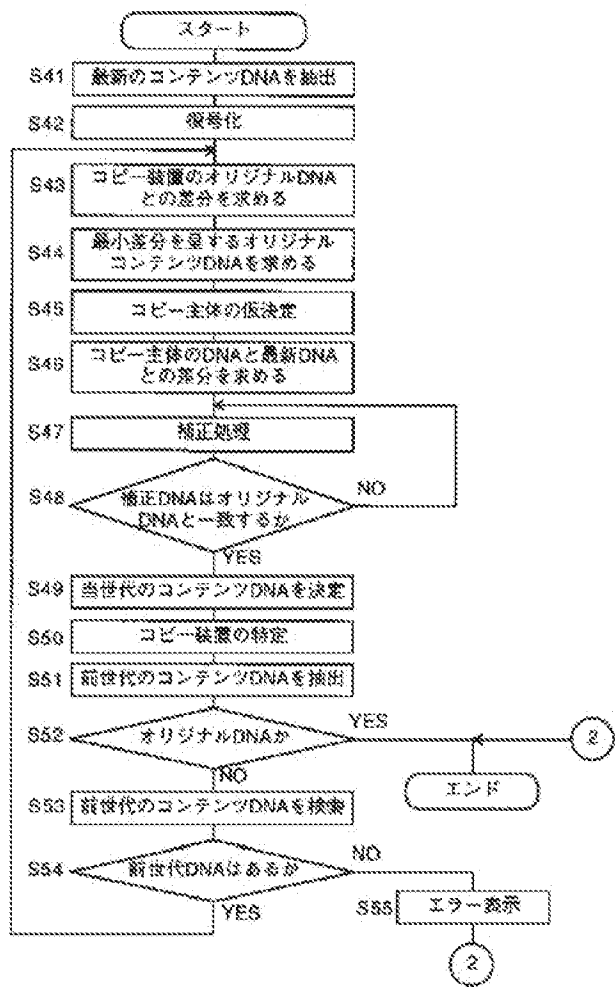


81	82	83	84	85	86	87	88	89	90	91	92
コンテンツ ID 1	コピー 領域 ID 1	コピー 領域 ID 11	コピー 領域 ID 2	コピー 領域 ID 12	コピー 領域 ID 4	コピー 領域 ID 14	コンテンツ ID 2	コンテンツ ID 3	コピー 領域 ID x	コピー 領域 ID 5	コピー 領域 ID 15
83			84			85			86		

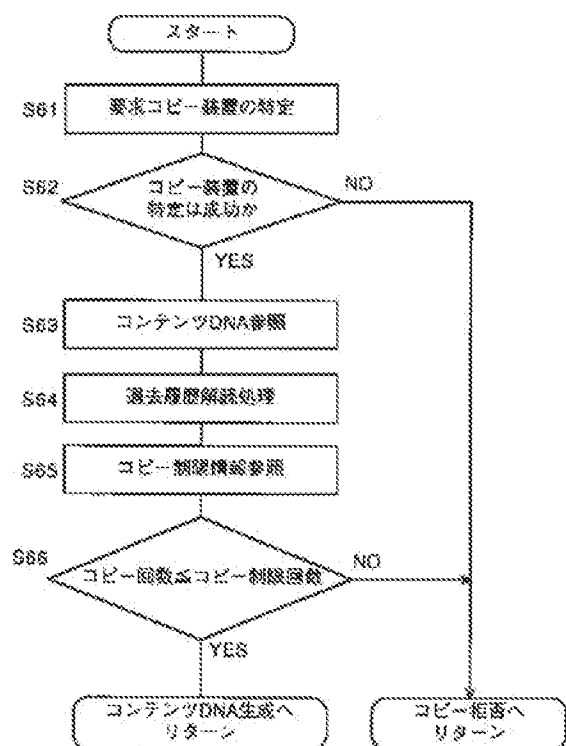
[Drawing 8]



[Drawing 10]



[Drawing 12]



[Translation done.]